EXPERT REPORT OF BRUCE W. PIXLEY

INTRODUCTION AND SUMMARY OF KEY FINDINGS

1. I have been retained by Quarles & Brady LLP, counsel for defendant Jessica Grailer, in the matter of *ECOLAB Inc., and NALCO COMPANY, LLC d/b/a Nalco Water, an Ecolab Company and/or Nalco Water v. Jessica Grailer*. I have been asked to review the report of Laurence Lieb, along with the digital evidence provided in this matter.

2. Mr. Lieb expresses two principal opinions in his report. One is that Jessica Grailer copied various files to a USB thumb drive that Mr. Lieb says Ms. Grailer connected to her Ecolab laptop at 9:39:51 PM (CST) on January 8, 2023. The other is that, after returning her Ecolab laptop on January 10, 2023, Ms. Grailer used a different computer to access Ecolab's network and then access and delete Ecolab files. I conclude that those opinions, as well as other opinions of Mr. Lieb's that I also address below, have no basis in evidence. Instead, evidence that Mr. Lieb systematically excluded from his report decisively refutes them.

3. Mr. Lieb's claim that Ms. Grailer connected her USB thumb drive and copied files to it on January 8, 2023, is clearly false on three different grounds.

4. First, Ecolab's data loss protection tool, Digital Guardian, was monitoring Ms. Grailer on January 8, 2023, and produced a report that would have recorded it if Ms. Grailer had copied files to her thumb drive that day. That is exactly what Digital Guardian is meant to do. Mr. Lieb reviewed the Digital Guardian report that tracked Ms. Grailer's activities, but he was silent in his own report about what the Digital Guardian report said. As he later admitted in his deposition, this was because Digital Guardian did *not* record Ms. Grailer copying *any* files to her USB thumb drive on January 8, 2023. Digital Guardian made a record of Ms. Grailer's activities throughout January 8, 2023. That record shows that Ms. Grailer did not copy even one of the hundreds of files that Mr. Lieb claims Ms. Grailer copied to her thumb drive on January 8, 2023. Mr. Lieb chose simply to omit this exculpatory evidence from his report.

5. Second, Mr. Lieb's narrative about Ms. Grailer's alleged activities on January 8, 2023, does not even make logical sense. On the one hand, Mr. Lieb opines (and he testified in his deposition) that Ms. Grailer connected her thumb drive to her laptop at exactly 9:39:51 PM (CST)

on January 8, 2023, and then began copying files to the thumb drive. On the other hand, when pressed for specific times at which he believes Ms. Grailer copied specific files to her thumb drive—details that Mr. Lieb conspicuously omitted from his report—Mr. Lieb always offers times *before* 9:39:51 PM (CST) on January 8, 2023. Mr. Lieb's conflicting statements add up to two mutually exclusive stories, neither of which is based on evidence, and one of which is also impossible. Story #1 is that Ms. Grailer connected her thumb drive to her laptop at 9:39:51 PM (CST) on January 8, 2023 and then began copying files. The most immediate, although not the only, problem with this story is that Mr. Lieb never identifies *any* files that he claims were copied at or after 9:39:51 PM (CST) on January 8. Story #2 is that Ms. Grailer copied hundreds of files to her thumb drive *before* Mr. Lieb claims that she connected the thumb drive to her computer at 9:39:51 PM (CST). That story cannot be reconciled with story #1, and it further implies that Ms. Grailer did something that cannot be done: copy files to a USB thumb drive that even Mr. Lieb does not claim was connected to the computer at the time (and do this without Digital Guardian recording it as well).

6. Third, the evidence is clear and overwhelming that Ms. Grailer last connected and disconnected her thumb drive to and from the computer on December 20, 2022. The act of connecting and disconnecting a thumb drive causes numerous time stamps to update in the Windows operating system, including in event logs that record and can clearly report connection and disconnection histories for USB storage devices such as Ms. Grailer's thumb drive. Those time stamps, which can be accessed using two competing software tools and cross-validated against one another, provide layers of evidence proving that Ms. Grailer last connected and disconnected her thumb drive on December 20, 2022. For example, Exhibits D-6 and D-8 to this report, both of which I will address in more detail below, contain Widows event logs clearly showing that Ms. Grailer connected and disconnected her thumb drive on different days up through December 20, 2022—and then never again. As the event logs show, the next time anyone connected an external USB storage device to the computer was when Mr. Lieb did so on February 8, 2023. Mr. Lieb testified in his deposition that he knew that the event logs, as well as many other time stamps, were relevant and available to him. But although the event logs, along with

multiple other time stamps which validate the event logs, all clearly show that Ms. Grailer last had her thumb drive connected on December 20, 2022, Mr. Lieb said nothing about this exculpatory evidence in his report. He omitted it despite testifying that he knew to look for it. Instead of objectively reporting the evidence available to him, Mr. Lieb reported and relied upon a single outlier time stamp that conflicted with all other available data and which, upon responsible review, obviously resulted from a system-level event in which hundreds of time stamps in one area of the Windows registry (most of which had no relationship to Ms. Grailer's USB thumb drive) simultaneously updated to the identical time of 9:39:51 PM (CST) on January 8, 2023. No experienced and objective examiner would make this mistake of blindly relying on a single time stamp that conflicted with all other available time stamps, let alone without acknowledging the conflicting time stamps' existence. But that is what Mr. Lieb did.

7. Mr. Lieb's second principal opinion, that Mr. Grailer used what Mr. Lieb calls an "undisclosed" computer to access Ecolab's network and to access and delete files after January 10, 2023, is similarly grounded in no evidence and is refuted by the evidence that exists. In this instance, Mr. Lieb did not even consider the available relevant evidence when reaching his conclusions. He formed his opinions about Ms. Grailer's post-January 10 activities based solely on his review of two pages of spreadsheet data that Plaintiffs provided to him, which Mr. Lieb admittedly did not even understand. Those two pages of spreadsheet data are shown in Exhibit D-22 to this report. Mr. Lieb admits that he did not even understand where that data had come from when he relied upon it make his accusations against Ms. Grailer. Plaintiffs gave Mr. Lieb a heavily filtered extract from a much larger volume of audit log data available to them. But by his own account, Mr. Lieb (i) incorrectly believed the data had come from Digital Guardian (which it clearly had not); and (ii) failed to realize that the spreadsheet he'd received was part of an audit log that was missing nearly all available columns of data. Nonetheless, Mr. Lieb proceeded to reach conclusions based on what appeared in the two-page spreadsheet he did not understand. And he did so by jumping to conclusions that the spreadsheet did not even support. For example, based on rows in the spreadsheet referencing "HardDelete" events, Mr. Lieb jumped to the incorrect conclusion that such rows showed Ms. Grailer deleting Ecolab's files. Similarly, based

on rows depicting "FilePreviewed" events relating to certain files, Mr. Lieb jumped to the incorrect conclusion that the rows showed Ms. Grailer not only "previewing" files, but somehow accessing and taking possession of them.

8. Nothing about Mr. Lieb's approach was reasonable or sound. An experienced and objective examiner will not simply make assumptions based on data that a party has filtered and which the examiner does not understand. And here, the audit log data that Mr. Lieb failed to obtain on his own—data that, to my understanding, Plaintiffs did not make available until Ms. Grailer moved the Court to compel them to produce it—ultimately demonstrated that Mr. Lieb's uninformed conclusions were incorrect. The audit log data that Plaintiffs produced in response to Ms. Grailer's motion, which Mr. Lieb for some reason *still* declined to consider when preparing his report, shows that Ms. Grailer never logged into her Ecolab Microsoft account after January 8, 2023. She was not even logged in on the days when Mr. Lieb claimed, without reviewing the available evidence, that she was accessing the account. The "HardDelete" log entries that Mr. Lieb speculated would show Ms. Grailer deleting files turned out to reflect the mere deletion of Outlook calendar events on the calendars of other employees who had granted Ms. Grailer access to their calendars. And the "FilePreviewed" events that Mr. Lieb speculated would show Ms. Grailer accessing and taking possession of files turned out to reflect a Microsoft application called PeoplePredictions displaying thumbnail images of files in Ecolab's Sharepoint cloud service from a Microsoft IP address in Iowa. None of that activity had anything to do with Ms. Grailer accessing her Ecolab Microsoft account, let alone accessing files. As shown by the log data that Mr. Lieb did not see fit to obtain and consider, Ms. Grailer never logged into that account after January 8.

9. I will explain these key findings in the Detailed Analysis and Findings Section below, along with my findings about other related errors that Mr. Lieb made throughout his report.

PROFESSIONAL CREDENTIALS AND QUALIFICATIONS

10. I am the Managing Member of Pixley Forensics Group LLC. My responsibilities include assisting corporate clients and law firms in investigations and disputes involving forensic

accounting issues, electronic discovery, theft of intellectual property, and computer forensic investigations. In this capacity, I manage teams of forensic examiners and use a variety of technologies to perform data acquisition and analysis of this information.

11. I started working in the field of computer forensics as a Santa Barbara Sheriff's Sergeant in 1999 when I was assigned to supervise and investigate high-tech crime.

12. Starting in 2001, I served as a lead instructor of computer forensics, Internet investigations, and network intrusion courses for the California Department of Justice's Advanced Training Center. Additionally, I have been employed as a Master Instructor at Guidance Software, which developed the EnCase computer forensic software. As an instructor, I have taught for over 2,000 hours on the subjects of computer forensics and high-tech investigations. I have developed course training materials and wrote manuals for computer forensic courses such as Advanced Internet Examinations and Network Intrusion Investigations.

13. I possess three professional certifications for my fields of work. I possess the Certified Information Systems Security Professional (CISSP) certification and the GIAC Certified Forensic Analyst (GCFA) certification, which are both ANSI ISO accredited credentials, and the EnCase Certified Examiner certification.

14. Since 2003, I have been retained as a computer forensic examiner and subject matter expert in both criminal and civil matters. I have been qualified as an expert witness in both state and federal courts and testified about the foundation of computer forensics, Windows and Mac operating systems, chat software, Internet and network operations, e-mail, peer-to-peer file sharing, digital photography, recovery of deleted data, and Trojan viruses.

15. Attached as **Exhibit A** to this declaration is a copy of my current Curriculum Vitae, which sets forth in detail additional aspects of my qualifications and background.

EVIDENCE CONSIDERED

16. I considered the following information in forming my opinions, in addition to other information cited in my analysis below:

a. Lieb Rule 26 Expert Witness Report dated November 13, 2023, including its Exhibits A–G.

b. Lieb Declarations dated February 21, 2023 and March 29, 2023 (including their exhibits).

c. On April 24, 2023, I received an external hard drive containing the following items: (i) a copy of a forensic image of the Ecolab HP laptop internal solid state drive ("Grailer Laptop") assigned to Ms. Grailer ("Grailer Image"); and (ii) a copy of Mr. Lieb's Axiom case files ("Axiom Case"), which indicates that Axiom version 6.10 was used to process the forensic image;

d. On May 4, 2023, I received a copy of the Digital Guardian report that reflected the user activity of the EcoLab laptop computer assigned to Ms. Grailer. This report was emailed from Plaintiff's counsel, James Hux, to Defendant's counsel as an email attachment (export_1194arc01-ecolab_2022-11-14_JG.xlsx) on May 3, 2023 and the attachment has a MD5 hash value of 035A9CCEB950DF57117D7EA744133D21;

e. On May 4, 2023, I also received a copy of an Excel file titled "JGrailer.xlsx." That Excel file was attached to the same email from Plaintiff's counsel, James Hux, referenced above;

f. On August 16, 2023, I received a copy of the Microsoft Office 365 audit logs ("O365 Audit Log") that reflected Ms. Grailer's account activity for the period of January 8 through January 18, 2023. The O365 Audit Log was emailed from Plaintiff's counsel, James Hux, to Defendant's counsel as an email attachment (O365 Logs for Grailer.xlsx) on August 16, 2023 and the attachment has a MD5 hash value of 1A4B4194914C933AC92A96E1D284E7E5;

g. Ms. Grailer's declarations dated March 8, 2023 and March 15, 2023 (including exhibits);

h. On January 23, 2024, I observed the deposition of Laurence Lieb taken by Defendant's counsel, and I reviewed the exhibits to Mr. Lieb's deposition; and

i. I also received a set of Mr. Lieb's invoices dated March 29, 2023 through July 13, 2023.

DETAILED ANALYSIS AND FINDINGS

I. LIEB'S ALLEGATION THAT GRAILER COPIED FILES ON 1/8/23

17. In his report, Mr. Lieb opines (i) that "Jessica Grailer last connected an Emtec 32GB, serial number 070B4A71ADB22353, USB Drive ('Emtec Drive') to her Ecolab Laptop on 1/8/2023 9:39:51 PM"; (ii) that "259 exfiltrated files [which Mr. Lieb lists by file name in Exhibit E to his report] were copied by Jessica Grailer to the Emtec Drive on January 8, 2023"; and (iii) that Ms. Grailer also copied other "files and folders to the Emtec Drive on January 8, 2023 in addition to the files described in [Mr. Lieb's] Exhibit E." (Lieb Report ¶¶ 17–19.)

18. Before I go on to address the evidence relating to these expressed opinions, I must note that based on his deposition, Mr. Lieb's opinions are not even coherent and logical. In his report, Mr. Lieb declined to identify the *times* at which he claims that Ms. Grailer exfiltrated files on January 8, 2023. That resulted in uncertainty about what exactly Mr. Lieb was claiming. And Mr. Lieb made that uncertainty worse, not better, during his deposition.

19. As noted above, Mr. Lieb opined in his report that Ms. Grailer last connected her USB thumb drive to her computer at 9:39:51 PM on January 8, 2023. Mr. Lieb did not (and does not) identify any other time that day that he claims the thumb drive was connected. This would imply that, in Mr. Lieb's view, Ms. Grailer must have exfiltrated files *after* 9:39:51 PM on January 8, 2023, since Ms. Grailer obviously could not have copied files to a thumb drive *before* connecting it. In a February 2023 declaration, however, Mr. Lieb testified that Ms. Grailer copied files to her thumb drive at specific times—and all those times were *before* 9:15 PM on January 8, 2023. (Lieb Decl. ¶¶ 24, 30–33, February 21, 2023.) Further, Mr. Lieb's report did not address this inconsistency. In his report, Mr. Lieb simply omitted all references to the specific "exfiltration" times he had included in his declaration.

20. Mr. Lieb also did not clarify his opinions during his deposition. When asked about the specific "exfiltration" times he'd provided in his February 2023 declaration (all before 9:15 PM on January 8, 2023), Mr. Lieb agreed that that was his testimony. (Lieb Dep. at pp. 91–96, Jan. 23, 2024.) During his deposition, he also testified that Exhibit F to his report contains evidence "consistent with" exfiltration on January 8, 2023 at specific times that again were before

9:15 PM. (Lieb Dep. at pp. 77–82.) At other points in his deposition, however, Mr. Lieb testified that in his opinion, Grailer did not begin "exfiltrating" files *until* 9:39:51 PM on January 8, 2023—when Mr. Lieb claims she connected her USB thumb drive. (Lieb Dep. at pp. 37–38, pp. 66–72, pp. 255–260, pp. 290–293, & Ex. 26.)

21. Mr. Lieb's inconsistencies and lack of clarity is a major red flag and enough on its own to tell an experienced and objective examiner that Mr. Lieb's analysis is not sound. Before feeling comfortable concluding that a user copied files to a USB thumb drive, an experienced and objective examiner would build an evidence-based timeline or chronology identifying the material events relating to that copying. That timeline would necessarily begin with the user connecting the thumb drive to the computer. Then, there would be specific subsequent times at which the user copied each file to the thumb drive. Finally, the timeline would end with the user removing the thumb drive from the computer after files had been copied to it. This is a basic thing that an examiner should be able to do if the examiner's conclusions are grounded in evidence and tell a story that is coherent and plausible. But Mr. Lieb has not provided a coherent timeline or chronology here.

22. The incoherence of Mr. Lieb's claims puts the person reviewing his work in the difficult position of genuinely not knowing what Mr. Lieb is claiming. In his declaration and even again during his deposition, Mr. Lieb testified that, in his opinion, Ms. Grailer "exfiltrated" files to her thumb drive at specific times that were all before 9:15 PM on January 8, 2023. But I do not know how to reconcile that testimony with (i) the fact that 9:39:51 PM is the only time at which Mr. Lieb claims Ms. Grailer connected her thumb drive on January 8, 2023 (and the fact that Ms. Grailer obviously could not have copied files to her thumb drive *before* connecting it); and (ii) Mr. Lieb's testimony during his deposition that Grailer did *not* begin "exfiltrating" files until she allegedly connected her thumb drive at 9:39:51 PM on January 8, 2023. Further adding to the confusion, Mr. Lieb has never identified a single specific "exfiltration" event, either in his declaration or his report, that he claims occurred *after* 9:39:51 PM. The upshot is that a reviewer in my position is unable to piece together Mr. Lieb's story. Mr. Lieb has asserted two mutually

exclusive positions—that all the "exfiltration" he alleges occurred *before 9:15 PM*, but also that it all occurred *after 9:39:51 PM*—and his narrative does not make sense.

23. I will now move on to address what the evidence shows in relation to Mr. Lieb's allegations. The reader, however, should keep in mind that we are not in the ordinary situation of having a coherent timeline or chronology to evaluate. Mr. Lieb has been extremely unclear about what that timeline is supposed to look like. It can be difficult to evaluate allegations if the person making them does specify the allegations you are trying to assess.

24. Even setting aside those serious problems, Mr. Lieb's expressed opinions are easily refuted by evidence that was available to Mr. Lieb, but which he omitted from his report and earlier declarations. As a preliminary matter, the Digital Guardian report for Ms. Grailer's Ecolab laptop was intended to record exactly the sort of copying that Mr. Lieb claims occurred. But that report refutes rather than corroborating Mr. Lieb's opinion that Ms. Grailer copied files to her USB thumb drive on January 8, 2023. Specifically, the Digital Guardian report records Ms. Grailer copying two files to her Emtec USB thumb drive on December 20, 2022—and never copying anything to that USB thumb drive (or to any other external storage media) again. The Digital Guardian report thus directly contradicts Mr. Lieb's expressed opinions about Ms. Grailer's January 8 activities. Mr. Lieb stated in his report that he had analyzed the Digital Guardian report, and he even acknowledged the Digital Guardian report's importance. But he never discussed any of the Digital Guardian report's contents in his own report, and he did not acknowledge that it contradicted his conclusions.

25. In addition, information in the Grailer Image conclusively shows that Ms. Grailer last had her Emtec USB thumb drive connected to her laptop on December 20, 2022. Ms. Grailer could not have copied files to her Emtec USB thumb drive on January 8, 2023, if she never connected that device to her laptop after December 20, 2022. But evidence in the Grailer Image uniformly identifies December 20, 2022 as the date Ms. Grailer last had her USB thumb drive connected, consistent with the Digital Guardian report's demonstration that Ms. Grailer last copied files to her USB thumb drive on December 20, 2022. The evidence showing that Ms. Grailer's USB thumb drive was last connected on December 20, 2022 is voluminous, permitting

an examiner to validate the December 20, 2022 date with multiple information sources. Mr. Lieb must have reviewed at least some of that evidence showing December 20, 2022 as the correct date. But as with the Digital Guardian's contents, Mr. Lieb said nothing about that exculpatory evidence in his report or earlier declarations.

26. My analysis in this Part I is broken into three sections. In Section A, I review what the Digital Guardian report shows in regard to Ms. Grailer's activities on January 8, 2023. Then, in Section B, I address the evidence in the Grailer Image pertaining to when Ms. Grailer last had her USB thumb drive connected to the laptop. That section itself is divided into many sub-sections, as I explain near the top of Section B. Finally, in Section C, I address other evidence that Mr. Lieb cites in support of his "copying" conclusion.

A. THE DIGITAL GUARDIAN REPORT

27. In his report, Mr. Lieb acknowledged not only that the Digital Guardian report is material evidence, but that Digital Guardian was specifically designed to capture the sort of copying that Mr. Lieb claims Ms. Grailer engaged in on January 8. Mr. Lieb stated that he based his report in part on "Ecolab's digital loss prevention tool, Digital Guardian, and related report that captures Jessica Grailer's human interaction with Ecolab's files." (Lieb Report ¶ 7.) He also stated that "Ecolab employs a data loss prevention tool, Digital Guardian, to journal Ecolab employees' interactions with Ecolab files, specifically to capture and memorialize unauthorized exfiltration of files, such as ***the downloading and copying of Ecolab files to external USB media***, uploading of Ecolab files to non-Ecolab cloud storage services, and the emailing of Ecolab files to third party email accounts." (Lieb Report ¶ 12 (emphasis added).) He further stated that "Digital Guardian is designed specifically to record the exfiltration of company files by employees." (Lieb Report ¶ 12.)

28. Mr. Lieb, however, never discussed any of the Digital Guardian report's contents in his report. He did not include any portion of the Digital Guardian report as an exhibit, and he never acknowledged what the Digital Guardian Report shows in terms of Ms. Grailer copying any files to external storage media. Mr. Lieb is correct that endpoint software such as Digital Guardian is designed to provide detailed records that track a user's activity, including the copying

of files to external storage devices. In fact, since the Windows operating system does not maintain a log of files that are copied to external storage media, the Digital Guardian report is the best evidence of whether and when any files were "exfiltrated." Mr. Lieb, however, completely omitted the Digital Guardian report's contents from his report.

29. I reviewed the Digital Guardian report. It contains many important details related to Ms. Grailer's activity. Since Mr. Lieb provided none of that information in his report, I will provide it here.

30. The Digital Guardian report is an Excel spreadsheet that contains a total of 253 possible fields of information for every recorded event. While not every field is used for each event (some are blank and not applicable), each event contains a significant amount of information for analysis. Because the Digital Guardian report is in Excel format, it can be easily filtered to show exactly which files Ms. Grailer copied to any external storage media, when she did so, and which device or devices she copied them to.

31. When I reviewed the Digital Guardian report, I found that it identifies only two events during the entire period from November 14, 2022 through January 8, 2023 when Ms. Grailer copied any files to any external storage media. Both those events occurred the morning of December 20, 2022.

32. Attached hereto as **Exhibit B-1** is data from the Digital Guardian report regarding the two events where Ms. Grailer copied files to external storage media. Exhibit B-1 displays eight of the 253 possible fields of information available for each event:

a. User (Ms. Grailer);

b. Event date and time;

c. Destination file path (where was the file copied to);

d. File size;

e. Source directory (where was the file copied from);

f. Operation type (stating that the user copied a file);

g. Destination device serial number (the serial number of the USB device the file was copied to); and

h. Computer name (the Ecolab computer assigned to Ms. Grailer).

33. The "Destination Device Serial Number" field in Exhibit B-1 confirms that the USB thumb drive Ms. Grailer was using on December 20, 2022 is the same drive that Mr. Lieb claims Ms. Grailer copied files to on January 8, 2023. The serial number (070B4A71ADB22353) is a match.

34. The Digital Guardian report contains no other entries for any files being copied to Ms. Grailer's USB thumb drive—or to any other external storage media.

35. The Digital Guardian report contains 80 entries for events on January 8, 2023. None of those entries were related to files being copied to any USB thumb drive or any other external storage media. The majority of the January 8 entries were related to email activity.

36. I examined the email stored in the Grailer Image and found that on January 8, 2023, Ms. Grailer used Outlook to send two email messages from her laptop:

a. An email dated January 8, 2023, at 7:55 PM, to David Lucas (dlucas@ecolab.com) with a CC to Joshua Galliart (jagalliart@ecolab.com) with a subject line of "Cargill – Puris Follow Up," and a single email attachment. This email was directed only to Ecolab recipients.

b. An email dated January 8, 2023, at 8:50 PM, to Joshua Galliart (jagalliart@ecolab.com) with a subject line of "Follow Ups," and nine email attachments. This email was directed only to one Ecolab recipient.

37. Of the 80 entries listed for January 8, 2023, 50 of those entries were related to granular activity associated with sending these two email messages and the attachments. When someone opens an attachment or adds an attachment to an email message, that attachment is copied to the InetCache folder (in this case, \Users\JLGRAILER\AppData\Local\Microsoft\Windows\InetCache). The InetCache folder is a hidden folder that is not managed by the user and this activity occurs behind the scenes. That activity was captured in the Digital Guardian report, along with Ms. Grailer's activity of sending the completed emails from Outlook. Ms. Grailer's emails messages on January 8 will also be addressed in a different section below.

38. The Digital Guardian report's remaining 30 entries for January 8, 2023 were related to web browser activity. These events were based on the logging of the Chrome and Edge browsers, and none list or describe files that were exfiltrated, whether by being copied to a USB thumb drive or otherwise.

39. Because the Digital Guardian report contains entries for only two files being copied to external storage media, both on December 20, 2022, it contradicts rather than supporting Mr. Lieb's expressed opinion that hundreds of files were "exfiltrated" to Ms. Grailer's Emtec USB thumb drive on January 8, 2023 (Lieb Report ¶¶ 17–19.) The Digital Guardian report would have captured such copying if it had occurred. That is precisely what Digital Guardian is designed to do. Instead, the Digital Guardian report shows that no files were copied to any external storage media after December 20, 2022. Mr. Lieb, however, did not even discuss that fact in this report.

40. When Mr. Lieb was asked about the Digital Guardian report at his deposition, he acknowledged that it contains no evidence of Ms. Grailer exfiltrating files on January 8, 2023. When asked why the Digital Guardian report did not capture the exfiltration that he alleges in his report, Mr. Lieb testified that the Digital Guardian report "cuts off at a time before those acts occurred." (Lieb Dep. at pp. 25–26.) The Digital Guardian report's final entry is time stamped 9:28 PM on January 8, 2023. Mr. Lieb testified that Ms. Grailer "may not have been connected to the internet" after 9:28 PM on January 8, and that the Digital Guardian agent running on her laptop therefore may not have been able to report logs about Ms. Grailer's post-9:28 PM activities back to Plaintiffs' server. (Lieb Dep. at pp. 33–34.)

41. This explanation that Mr. Lieb offered for the first time at his deposition again brings us to significant red flags. One red flag is that, during his deposition, Mr. Lieb testified that he could not recall analyzing whether Ms. Grailer was or was not connected to the Internet after 9:28 PM on January 8, 2023. (Lieb Dep. at pp. 34–37.) Similarly, Mr. Lieb testified that he did not perform any analysis to try to determine why the Digital Guardian report did not record any of the copying that he alleges. (Lieb Dep. at pp. 38–39.) That is problematic. An objective and experienced examiner would conduct analysis to understand and resolve countervailing evidence.

An objective and experienced examiner would not just assume that the lack of an Internet connection explains away countervailing evidence without undertaking the obvious first step of analyzing whether there *was* any lack of an Internet connection at the relevant time.

42. In fact, the evidence available in the Grailer Image and in Mr. Lieb's Axiom Case shows the Grailer Laptop disconnecting from Ecolab's network at 1:05 AM (CST) on January ***9***, 2023, several hours after Mr. Lieb speculated that the connection might have been terminated. (As discussed more below, Mr. Lieb's "Axiom Case" is the database—or "case"—that Mr. Lieb created when he used Axiom software to extract and analyze information from the image of Ms. Grailer's laptop.) This is depicted in the figures in **Exhibit B-2**, attached hereto. Mr. Lieb's speculation was simply wrong.

43. A second red flag is that Mr. Lieb's speculation about the laptop's Internet connection, even if it had any basis, would not explain anything to the extent Mr. Lieb alleges that Ms. Grailer copied files to her USB thumb drive *before* 9:28 PM on January 8. As noted above, Mr. Lieb may be making such a claim, although he is not clear about it. When asked about this at his deposition, Mr. Lieb testified that he "[does not] know" and has "no explanation" as to how Ms. Grailer could have copied files to her USB thumb drive before 9:28 PM on January 8 without Digital Guardian recording that activity. (Lieb Dep. at pp. 81, 87.)

44. A third red flag is that Mr. Lieb did not address any of these matters in his report, or in the declarations he filed with the Court. An experienced and objective examiner in Mr. Lieb's position would have acknowledged that the Digital Report provided countervailing evidence of Ms. Grailer *not* copying files to her USB thumb drive on January 8, 2023, and would have explained the evidence-based grounds, if any, for rejecting that countervailing evidence. Mr. Lieb did not do this in his declarations or his report. He did not even take the first step of admitting that the Digital Guardian report contradicted his conclusions. During his deposition, Mr. Lieb testified that he "would have reported" it if the Digital Guardian report had contained evidence of exfiltration—and that he left it out of his report *because* it contained no evidence of exfiltration. (Lieb Dep. at pp. 35, 70, 81–82.) That is not appropriate. An experienced and

objective examiner would not handle exculpatory evidence by simply declining to report that it exists.

45. There is one final issue to note before I turn away from the Digital Guardian report. In addition to the other problems discussed above, it is apparent that Mr. Lieb did not understand Digital Guardian when he executed his first declaration in February 2023. In that declaration, Mr. Lieb called the Digital Guardian report a report "of all interactions former employee Jessica Grailer performed regarding Ecolab files during the period November 14, 2022 through January 18, 2023 inclusive," and testified that he had "forensically analyzed the Digital Guardian Report and came to the forensic observations and opinions set forth in" his declaration. (Lieb Decl. ¶ 15, February 21, 2023.) He also claimed that the Digital Guardian report recorded specific events on January 14 and 15, 2023. (Lieb Decl. ¶¶ 14–17, February 21, 2023.) Those statements were plainly incorrect, in two different respects. First, the Digital Guardian report did not record any activity after January 8, 2023. Second, it was not true that Mr. Lieb came to his opinions based on his analysis of the Digital Guardian report—as Mr. Lieb agreed during his deposition, the Digital Guardian report never shows any of the "exfiltration" that Mr. Lieb alleges.

46. When asked about these discrepancies during his deposition, Mr. Lieb testified that when preparing his February 2023 declaration, he "assumed" that a separate spreadsheet file titled "JGrailer.xlsx" (which is discussed below) was also "from Digital Guardian," but that he later learned it "actually is not a Digital Guardian report." (Lieb Dep. at pp. 88–91, 103.) This suggests a worrisome lack of understanding about Digital Guardian. An experienced examiner would never mistake the "JGrailer.xlsx" spreadsheet for a Digital Guardian output. It looked nothing like (and contained far fewer data fields than) a Digital Guardian report, and it also covered a period of time *after* Ms. Grailer returned the laptop to Plaintiffs (whereas Digital Guardian was recording Ms. Grailer's activity on that laptop). No one who is familiar with Digital Guardian would have made the mistake that Mr. Lieb apparently made in the course of preparing his February 2023 declaration.

B. WHEN MS. GRAILER LAST HAD HER USB DRIVE CONNECTED

47. There is also a second reason Mr. Lieb cannot be correct in opining that Ms. Grailer copied files to her USB thumb drive on January 8, 2023. In addition to what the Digital Guardian report shows, many pieces of evidence from the Grailer Image demonstrate that Ms. Grailer never had her USB thumb drive connected to her laptop after December 20, 2022.

48. The analysis in this Section B will necessarily be more complex than that above regarding the Digital Guardian report. Digital Guardian is designed to provide information in a clear and readable format. That is not true for information that Windows stores relating to the connection and disconnection of USB devices. Such information is stored by Windows in different locations and for purposes that are operational rather than forensic. Forensic examiners can use software tools such as Axiom or OSForensics to extract the information, but that does not eliminate the need for careful analysis to verify each of the extraction software's outputs.

49. Accordingly, this section is broken into six subsections. In subsection 1, I provide general background about USB thumb drives and how the Windows operating system interacts with them. In subsection 2, I discuss information that the Windows registry stores about USB thumb drives in two registry "subkeys" that Windows calls "USBSTOR" and "USB." In subsection 3, I discuss additional information that Windows stores about USB thumb drives in two other locations: the Windows event logs and another registry subkey called "MountPoints2." In subsection 4—the longest subsection—I examine the information that was available to Mr. Lieb from all those sources in the Axiom Case that Mr. Lieb created when he used Axiom software to extract information from the Grailer Image. In subsection 5, I show how the information from Mr. Lieb's Axiom Case can also be validated by using a competing extraction software tool called OSForensics, which is sold by a developer called PassMark. Finally, in subsection 6, I discuss a bug in the Axiom software that resulted in one erroneous output in Mr. Lieb's Axiom Case. That erroneous output should not be problematic for an experienced and objective examiner—it was easily invalidated using the tools Axiom itself makes available for purposes of verification—but I address it here because it appears to have been an issue in Mr. Lieb's analysis.

1. USB THUMB DRIVES

50. Here I will outline the actions of the operating system when a USB thumb drive is connected to a Windows computer such as the Grailer Laptop. This understanding will provide the framework to know where the data is located and where forensic software, such as Axiom or OSForensics, should extract the information.

51. Every USB device, whether it is a thumb drive, external hard drive, keyboard, or mouse, is built to specs created by the USB Implementers Forum (USB-IF). Each USB device has a controller chip that is encoded by the device manufacturer with different information. One of those blocks of information is called the "device descriptor"[1] and it contains some key information that Windows[2] extracts when the device is inserted. Examples of this information, which will be covered throughout this report, include the following fields:

a. idVendor;

b. idProduct;

c. bcdDevice;

d. iManufacturer;

e. iProduct; and,

f. iSerialNumber.

52. Each time a USB thumb drive is connected to a Windows computer, the operating system will track information related to the connection and disconnection of that device. The Windows operating system primarily tracks this activity in two areas, the Windows registry[3] and Windows event logs.

---

[1] See table 9-11 in Universal Serial Bus 3.2 Specification, Revision 1.1, June 2022, https://www.usb.org/documents

[2] https://learn.microsoft.com/en-us/windows-hardware/drivers/ddi/usbspec/ns-usbspec-_usb_device_descriptor

[3] The Windows registry consists of multiple files that Microsoft refers to as "hives." These hives contain a hierarchy of information and settings that are organized for the functions of the operating system. As a simple example, a user may have a specific photo that is displayed as wallpaper on the user's desktop and that setting is in the registry.

2. WINDOWS REGISTRY – USBSTOR AND USB SUBKEYS

53. The first time a USB thumb drive is connected to a Windows computer, the operating system will automatically add information to the System hive of the Windows registry. A USB thumb drive fits into two categories of devices being tracked by the operating system: (i) USB storage devices; and (ii) USB devices generally (both storage and non-storage). Thus, the operating system will add information for one USB thumb drive to two main subkeys[4] in the registry, under the ControlSet001\Enum subkey:

a. the "USBSTOR Subkey," which is dedicated to USB storage devices; and

b. the "USB Subkey," which is dedicated to all USB devices.

54. The USBSTOR Subkey, which is located in the registry at ControlSet001\Enum\USBSTOR, contains an entry for each USB storage device. **Exhibit C, Figure 1** is a depiction of the USBSTOR Subkey in the System hive from the Grailer Image.

a. Below the USBSTOR Subkey is a new subkey hierarchy for the USB storage device (the "USBSTOR Device Subkey") which has a naming convention that lists the vendor name (iManufacturer), product name (iProduct), and revision number (bcdDevice). This subkey is outlined in green in Figure 1. For reference, the iManufacturer field for this device is empty and the iProduct field is "USB_DISK_2.0."

b. Below the USBSTOR Device Subkey is a further subkey that uses the internal USB serial number (iSerialNumber, 070B4A71ADB22353) as the subkey name. In Figure 1, the device's internal USB serial number tells us that we are looking at the same USB drive that Mr. Lieb discusses in his report.

c. Among other subkeys of the USBSTOR Device Subkey, there are four subkeys called 0064, 0065, 0066, and 0067, which are also depicted and outlined in red in Figure 1. These subkeys contain time stamp values relating to when different activities occurred:

[4] The hierarchy of the registry visually appears as a folder structure and Microsoft refers to each folder as a subkey.

i. The 0064 subkey contains a single time stamp[5] value indicating when the USB thumb drive was first plugged into the computer ("First Install Date/Time").

ii. The 0065 subkey contains a single time stamp value indicating when the driver for the thumb drive was activated. Since this occurs at the same time as 0064, it will be the same time.

iii. The 0066 subkey contains a single time stamp value indicating when the thumb drive was last plugged into the computer ("Last Insertion Date/Time").

iv. The 0067 subkey contains a single time stamp value indicating when the computer last detected that the thumb drive had been removed ("Last Removal Date/Time").

55. The USB Subkey, which is located in the registry at ControlSet001\Enum\USB, is similar. The USB Subkey again contains an entry for each USB device, which again includes Ms. Grailer's USB thumb drive. **Exhibit C, Figure 2** is a depiction of the USB Subkey in the System hive from the Grailer Image.

a. As with the USBSTOR Subkey, below the USB Subkey is a new subkey hierarchy for the USB thumb drive ("USB Device Subkey"). The USB Device Subkey, however, is slightly different from the USBSTOR Device Subkey described above. Instead of vendor name, product name and revision number, it lists the vendor's ID number (idVendor, VID 6557)[6] and product ID number (idProduct, PID 4200). This subkey is outlined in green in Figure 2.

b. Below the USB Device Subkey is a subkey that uses the internal USB serial number (iSerialNumber, 070B4A71ADB22353). This is the same serial number found in

---

[5] The time stamp is eight hex values that decode to a Windows time stamp, which Microsoft refers to as FILETIME. An example of FILETIME looks like this: E1 B4 F4 1E 56 DE D8 01. While it may not look like a time stamp, the value is a 64-bit integer that is the number of 100-nanosecond intervals since January 1, 1601 (reference https://learn.microsoft.com/en-us/windows/win32/sysinfo/file-times)

[6] The vendor ID is 0x6557. This ID is assigned to the vendor by the USB-IF. This vendor ID was assigned to Emtec.

the USBSTOR Device Subkey. It tells us that we again are looking at the USB drive that Mr. Lieb discusses in his report.

c. Just like in Figure 1, the USB Device Subkey in Figure 2 has four further subkeys called 0064, 0065, 0066, and 0067 (outlined in red). These will contain the same time stamps values as the corresponding 0064, 0065, 0066, and 0067 subkeys in the USBSTOR Device Subkey, as described above.

3. EVENT LOGS AND WINDOWS REGISTRY – MOUNTPOINTS2

56. As relevant here, there are two other places Windows stores information relating to when a USB device is connected and disconnected. First, in addition to the first and last time stamps for the activity of a USB thumb drive in the registry, the operating system creates event log entries[7] for each time that the USB thumb drive is connected and disconnected. These event log entries are very helpful because they provide, not only a snapshot of the last time a thumb drive was connected or disconnected, but a history of the device's connections and disconnections over time.

57. Second, the Windows registry includes yet another subkey, called the "MountPoint2 Subkey," that provides another reference of when a USB storage device was last connected to the computer. The MountPoints2 Subkey is associated with the user account[8] that plugged in the USB storage device. It contains a further subkey for each USB storage device that had been connected.

4. THE EVIDENCE IN MR. LIEB'S AXIOM CASE

58. Mr. Lieb created his Axiom Case on February 9, 2023, using Axiom version 6.10. Mr. Lieb's Axiom Case includes extracted information from all the sources I discussed above: the Windows registry USBSTOR Subkey and USB Subkey, the Windows event logs, and the

---

[7] These event log entries have an Event ID of 1006 and are stored in a specific event log: Microsoft-Windows-Partition%4Diagnostic.evtx. These events are created when a USB thumb drive is connected and detected as disconnected.

[8] Each Windows user profile contains a user profile hive, which is a system file called NTUSER.DAT. For Grailer, this was located in the \Users\JLGRAILER folder.

MountPoints2 Subkey. I will use Mr. Lieb's Axiom Case to review information from each of those sources in this subsection.

59. Before I do so, I note that Magnet Forensics, the developer of Axiom, urges examiners to verify rather than to blindly rely upon Axiom's reported outputs. Magnet Forensics maintains a webpage on its support website entitled "Artifact Profile: USB Devices." A copy of that webpage is attached hereto as **Exhibit D-1.** The page contains a section called "Verifying timestamps from USB devices," with the following language:

> *"Timestamps for USB devices are retrieved from the device registry, and due to the behavior of registry keys, may not always accurately reflect the true time when a user performed a certain action.*
>
> *Timestamp data for a registry key may update when any of the data within that key changes. In other words, if multiple timestamps are recovered from the same registry key, they may all inaccurately display the same timestamp, for example the one that was most recently recorded for that key*
>
> *For this reason, it's important to verify these timestamps with other USB-related artifacts, such as the modified date/time of a file stored on the USB device, or other timestamp data on the computer where the USB device was plugged in."*

60. Magnet Forensics also notes, in the same Exhibit D-1, that "typically you need to collect details from multiple locations to analyze USB activity on a Windows PC."

61. The above is relevant and sound advice from the vendor to forensic examiners using the vendor's software. Forensic software such as Axiom is designed to extract information from a forensic image so the examiner need not manually look for every piece of information. This automation is extremely helpful, but it is critical that the examiner knows how to verify the reported output of the forensic software—and to evaluate all the outputs that are relevant. A given output can be misleading if, for example, the software extracts the wrong information, or if it extracts the correct information but reports it incorrectly. Thus, despite benefiting from the software's automation, the examiner should know how to find the information manually. Further, there are circumstances when a single time stamp, even if correctly reported by the forensic

software, may not accurately reflect the true time when a thumb drive was connected or disconnected. Thus, the examiner must also compare the different outputs that the software extracts from different locations in the computer, and may also choose to use other forensic software for further comparison.

62. I will follow these principles in my analysis below. Mr. Lieb did not follow them in his. Mr. Lieb testified during his deposition that he knows that "[t]he act of connecting a USB drive to a Windows operating system will create timestamps in a variety of locations on a Windows laptop." (Lieb Dep. at p. 212.) He also testified that "That's why it's very difficult for a layperson to try and cover their tracks on a Windows computer because most people aren't aware that evidence of activity appears and is recorded in 20 different locations." (Lieb Dep. at p. 214.) But as we will see, Mr. Lieb relied on only one time stamp, from one location, to support his conclusion that Ms. Grailer connected her USB thumb drive at 9:39:51 PM on January 8, 2023. He omitted all the other relevant time stamps from his report, never mentioning that they all showed Ms. Grailer last connecting and disconnecting her thumb drive on December 20, 2022.

63. Mr. Lieb further did not follow his own "best practice" of validating the outputs from a software tool like Axiom by testing them against the outputs from a competing tool such as OSForensics. During his deposition, Mr. Lieb testified as follows:

> *"Q. [B]oth Axiom and OS Forensics extract and report timestamp information from multiple sources in Windows, right?*
>
> *A. The reason I personally used two tools on the same evidence is that almost every single case, the two different tools, they're highly respected, they're used by US law enforcement and US military, will extract the same and report on the same evidence and in one tool it will extract and report on evidence – or Axiom will extract and identify evidence that OS Forensics does not, and vice versa. OS Forensics will extract. So my best practice is not just run one tool. I like to – I always create two different cases and the two different tools, see where the overlap is, and then look to see what is one tool reporting that the other is not, and then dig into that; go, okay, Axiom identified this information, I'm not showing up in OS Forensics. I'm going to look into OS Forensics and*

> *see why it's not there. Sometimes I'll reach out to Passmark or – who's the owner or manufacturer of OS Forensics, and say, hey, you missed this. They'll update it for the next – and vice versa.*
>
> *Yeah, I can't explain it why. But some experts I've encountered say, oh, no, I can only use one tool. And I can prove that's not a good idea."*

(Lieb Dep. at pp. 218–219.)

As we will see, however, Mr. Lieb did not follow this practice. OSForensics allows the examiner to confirm, through multiple time stamps, that Ms. Grailer last connected her USB thumb drive on December 20, 2022. But Mr. Lieb omitted all those outputs from OSForensics in his report, just as he omitted all the time stamps in his Axiom Case that contradicted his conclusion.

Axiom's Section Regarding Connected USB Devices

64. Mr. Lieb's Axiom Case displays a section where an examiner can access information regarding USB devices that have been connected to the computer. **Exhibit C, Figure 3** is a depiction from that section of Mr. Lieb's Axiom Case.

65. Annotations from both Mr. Lieb and me appear in Figure 3. In the left hand column are yellow and purple rectangles. Those are Mr. Lieb's. The yellow rectangles indicate that Mr. Lieb flagged each of those rows as "of interest." In addition, I outlined two rows in red, and I outlined the serial number in each of those rows in yellow.

66. Both of the outlined rows in Figure 3 are for Ms. Grailer's Emtec USB thumb drive, the drive Mr. Lieb discusses in his report. We know this because of the matching serial number outlined in yellow.

67. Ms. Grailer's USB thumb drive appears twice in Figure 3 because, as I explained above, the Windows operating system tracked the device in two separate registry subkeys: the USBSTOR Subkey (for USB storage devices) and the USB Subkey (for all USB devices). The first outlined row is for the USBSTOR Subkey. The second outlined row is for the USB Subkey.

68. An experienced examiner would notice right away that Figure 3 provides different "last connected" time stamps for Ms. Grailer's USB thumb drive. Those time stamps should match, since they are for the same USB device. But they do not. The reported time stamp from

the USBSTOR Subkey is 12/20/2022 6:26:42 AM. However, the reported time stamp from the USB Subkey is 1/8/2023 9:39:51 PM. Since they are for the same device, these conflicting time stamps cannot both be correct.

69. Fortunately, Axiom enables the examiner to manually review the underlying values stored in the Windows registry. By selecting each of the highlighted rows, an examiner can navigate through Axiom to access those values. I will begin with the first outlined row, for the USBSTOR Subkey.

USBSTOR Subkey

70. When an examiner selects the first outlined row in Figure 3, Axiom displays more detailed "ARTIFACT INFORMATION" and "EVIDENCE INFORMATION." That information is depicted in **Exhibit D-2**, attached hereto, which is a full-page screenshot from Mr. Lieb's Axiom Case. The "ARTIFACT INFORMATION" appears in the upper part of the right-hand column. The "EVIDENCE INFORMATION" appears below that "ARTIFACT INFORMATION." For ease of reading, zoomed-in screenshots of the "ARTIFACT INFORMATION" and part of the "EVIDENCE INFORMATION" are also attached hereto as **Exhibit C, Figures 4 and 5**. I have outlined two entries in Figure 5 in red, for reasons I will explain below.

71. In Figure 4 (the "ARTIFACT INFORMATION") Axiom reports certain outputs for the USB thumb drive. (It also reports an Item ID of 484567. That Item ID is assigned to the entry by Axiom and is case specific.) The outputs in Figure 4 include a USB serial number (iSerialNumber), which again confirms we are looking at the same USB thumb drive discussed in Mr. Lieb's report. The outputs also include time stamps.

72. The "ARTIFACT INFORMATION" in Figure 4 lists the "First Install" time stamp for Ms. Grailer's USB thumb drive as 10/12/2022 11:17:28 AM (CDT); the "Last Insertion" timestamp as 12/20/2022 6:26:32 AM (CST); and the "Last Removal" timestamp as 12/20/2022 4:55:04 PM (CST). The "Last Insertion" timestamp is ten seconds earlier than the "Last Connected" time stamp of 12/20/2022 6:26:42 AM that we saw in Figure 3, which we also see again in Figure 4. I will address the "Last Connected" time stamp as well as the ten-second

difference that time stamp and the "Last Insertion" time stamp when I discuss the MountPoints2 Subkey below.

73. Turning to Figure 5—the "EVIDENCE INFORMATION"—we see the "Locations" from where Axiom extracted the information (including the time stamps) reported in Figure 4. This is an extremely important feature of Axiom that Mr. Lieb does not discuss in his report. By design, the hyperlinked entries in Figure 5 (shown in blue font) enable the forensic examiner to manually access and thus to verify the registry values that Axiom is attempting to report. The "Source" entry tells us the information is located in the System hive file in the Grailer Image. And below the word "Location," you can see additional hyperlinks to specific subkeys in the System hive. Those entries are hyperlinks by design. When the examiner clicks on them, Axiom will take the examiner to the specific subkeys in the registry, so the examiner can manually access the values stored in each of those subkeys.

74. I have outlined the fourth and fifth locations in Figure 5 in red. These are the hyperlinks for the 0066 subkey and 0067 subkey. As I explained above, the 0066 subkey stores the "Last Insertion" time stamp value, and the 0067 subkey stores the "Last Removal" time stamp value. I will navigate through each of those subkeys to see whether or not they validate the outputs reported in Figure 4.

75. When I click on the hyperlink for the 0066 subkey (Last Insertion), Axiom navigates to the 0066 subkey and displays the value name, value type, and value data depicted in **Exhibit C, Figure 6**. The value data is an 8-byte hex value for Windows FILETIME. That 8-byte hex value is the time stamp. As explained above, it is a number of 100-nanosecond intervals since January 1, 1601 (reference: https://learn.microsoft.com/en-us/windows/win32/sysinfo/file-times).

76. Axiom enables the examiner to decode the 8-byte hex value shown in Figure 6. The examiner can do this simply by highlighting the hex value. When I do so in Mr. Lieb's Axiom case, the time stamp is displayed in Coordinated Universal Time (UTC), as depicted in **Exhibit C, Figure 7**.

77. As seen in Figure 7, a "Last Insertion" time stamp value of 12/20/2022 12:26:32 PM (UTC) was decoded from the 0066 subkey. Converting from UTC to Central Standard Time

(UTC-6), that time stamp value is 12/20/2022 6:26:32 AM. This matches and thus validates the "Last Insertion" time stamp value that we saw in Figure 4.

78. For reference, attached hereto as **Exhibit D-3** is a full-page screenshot from Mr. Lieb's Axiom Case. Exhibit D-3 shows how the above decoding process looks to the examiner on the computer screen.

79. Now I will follow the same procedure to manually access and decode the "Last Removal" time stamp value in the 0067 subkey. When I click on the hyperlink for the 0067 subkey, Axiom navigates to the 0067 subkey and displays the value name, value type, and value data depicted in **Exhibit C, Figure 8**. Again, the value data is an 8-byte hex value for Windows FILETIME.

80. When I decode the 8-byte hex value in the same manner as above, Axiom displays it in UTC as depicted in **Exhibit C, Figure 9**. In UTC, the "Last Removal" time stamp is 12/20/2022 10:55:04 PM. Adjusting to Central Standard Time (UTC-6), that is 12/20/2022 4:55:04 PM. This matches and thus validates the "Last Removal" time stamp value that we saw in Figure 4.

81. The same decoding process can also be followed for the other two subkeys (0064 and 0065). I did that too. I manually decoded the time stamp values stored in those subkeys and confirmed that they also match the time stamps reported in Figure 4.

82. To recap, Axiom allowed me to manually access and decode the time stamp values stored in the USBSTOR Subkey. Doing so allowed me to validate the October 12, 2022 and December 20, 2022 time stamps reported in Figure 4. Mr. Lieb, however, never addresses any of these time stamps in his report. In fact, Mr. Lieb's report does not cite *any* evidence from the USBSTOR Subkey, even though Mr. Lieb flagged the USBSTOR Subkey for Ms. Grailer's USB thumb drive as "of interest" in his Axiom Case. Mr. Lieb testified during his deposition that he knows that connecting a thumb drive to a Windows operating system will create time stamps specifically in the USBSTOR Subkey (which Mr. Lieb called the "USBSTOR file" in his deposition). (Lieb Dep. at p. 212.) Nonetheless, he omitted all of the USBSTOR Subkey's time stamps from his report.

83. Before I move on the USB Subkey, I note for clarity that the "Last Removal" time stamp shown in Figure 4 (12/20/2022 4:55:04 PM CST) does not necessarily tell us when Ms. Grailer last physically removed the USB thumb drive from the computer. Instead, it tells us when the computer last detected the USB thumb drive's removal. Ms. Grailer could have physically removed the device at an earlier time. For example, if a USB thumb drive is removed while the computer is in sleep mode, the computer will not detect that removal until it is awake.

84. Here, the evidence tells us that Ms. Grailer did in fact remove her USB thumb drive from her laptop sometime before 12/20/2022 4:55:04 PM (CST). The computer then detected that removal when it resumed from sleep mode. The System event log[9] can be queried to determine when the computer is in sleep mode and awake. **Exhibit C, Figure 10** is a screenshot from Mr. Lieb's Axiom Case depicting the event log entries for the computer's sleep mode function on December 20, 2022. For reference, a full-page screenshot from Axiom that includes the depiction used in Figure 10 is also attached hereto as **Exhibit D-4**. Combined with the other evidence covered above, this event log information yields the following timeline:

a. As shown in Exhibit C, Figure 10, the computer resumed from sleep mode at 5:22:37 AM (CST) on December 20, 2022.

b. As shown in Exhibit C, Figure 4 (and validated manually above), Ms. Grailer's Emtec USB thumb drive (iSerialNumber 070B4A71ADB22353) was inserted at 6:26:32 AM (CST), while the computer was awake.

c. As shown in Exhibit B-1, the Digital Guardian report demonstrates that two files were copied to the Emtec USB thumb drive (serial number 070B4A71ADB22353) at 6:27:23 AM (CST), shortly after Ms. Grailer inserted the drive into the computer.

d. As shown in Exhibit C, Figure 10, the computer was placed into sleep mode at 6:28:23 AM (CST).

[9] Windows\System32\winevt\Logs\System.evtx

e. Figure 10 indicates the computer resumed from sleep mode at 4:55:05 PM (CST). However, I am able to use Mr. Lieb's Axiom Case to access the details for that event log entry, which show the precise wake time in UTC with nanoseconds as "2022-12-20T22:55:03.0467518Z." That equates to 4:55:03 PM (CST), two seconds earlier than the event log time value shown in Figure 10.

f. As shown in Exhibit C, Figure 4 (and validated manually above), the Emtec USB thumb drive (iSerialNumber 070B4A71ADB22353) was last detected as removed at 12/20/2022 4:55:04 PM (CST), one second after the precise time the computer resumed from sleep mode. This suggest the USB thumb drive had been removed while the computer was in sleep mode.

85. Notably, this evidence-based timeline coincides with the testimony Ms. Grailer provided in her second declaration (Grailer Decl. ¶¶ 36, 46–50 & Ex. C, March 15, 2023) regarding what she recalled about her activities on December 20, 2022. Plaintiffs had not yet given us access to the Digital Guardian report or the Grailer Image when Ms. Grailer provided that declaration. But the Digital Guardian report and the evidence discussed above from the Grailer Image turned out to corroborate the statements in Ms. Grailer's declaration.

USB Subkey

86. Now I will similarly use Mr. Lieb's Axiom Case to access the time stamp values stored in the USB Subkey. As a preliminary matter, however, I note that although the USB Subkey is the one location from which he actually reported a time stamp, Mr. Lieb testified during his deposition that he was "not familiar" with the USB Subkey at all. (Lieb Dep. at pp. 214–215.) This is another red flag regarding Mr. Lieb's analysis. An experienced examiner would be very familiar with both the USBSTOR Subkey and the USB Subkey. In addition, an experienced and objective examiner would not report a time stamp from a registry subkey without understanding what that subkey is.

87. I will begin my analysis of the USB Subkey by returning to Figure 3 and selecting the second outlined row in that figure. Similar to what we saw above, when an examiner selects the second outlined row in Figure 3, Axiom displays more detailed "ARTIFACT

INFORMATION" and "EVIDENCE INFORMATION." This is depicted in **Exhibit D-5**, attached hereto, which is a full-page screenshot from Mr. Lieb's Axiom Case. For ease of reading, zoomed-in screenshots of Exhibit D-5's "ARTIFACT INFORMATION" and "EVIDENCE INFORMATION" are also attached hereto as **Exhibit C, Figures 11 and 12**. As shown in Figure 11, the serial number confirms we are still looking at the same USB device.

88. The examiner should immediately notice in Figure 11 that Axiom is reporting the same output for the device's "First Install," "Last Insertion," and "Last Removal" time stamps. All three time stamps appear in Figure 11 as 1/8/2023 9:39:51 PM. This is also the time when Mr. Lieb opines that Ms. Grailer last connected her USB thumb drive to the computer. (Lieb Report ¶ 17.) Footnote 2 of Mr. Lieb's report tells us he obtained that time stamp from the information depicted in Figure 11, as I will also address in further detail below. (Lieb Report ¶ 17 n.2.) Mr. Lieb's report, however, did not acknowledge that in Figure 11, Axiom reported that Ms. Grailer's USB thumb drive was first installed, last inserted, *and* last removed all at that same time.

89. An experienced and objective examiner would quickly see two red flags suggesting that the 1/8/2023 9:39:51 PM time stamps in Figure 11 are not reliable. First, Ms. Grailer could not possibly have first installed, last inserted, *and* last removed her USB thumb drive from the laptop all at the same second. Second, the outputs reported in Figure 11 contradict the outputs that Mr. Lieb's Axiom Case provided from the USBSTOR Subkey in Figure 4, and above, I was able to verify those USBSTOR outputs by manually accessing and decoding the actual time stamp values stored in the USBSTOR Subkey.

90. Before reaching any conclusions, however, I will manually access and decode the time stamp values stored in the USB Subkey, just as I did above for the values stored in the USBSTOR Subkey. Mr. Lieb's Axiom Case allows me to do that by clicking on the evidence location hyperlinks shown in Figure 12 and navigating to decoded time stamps. I did so, and the results are as follows:

a. The 0064 subkey (**Exhibit C, Figure 13**) contains the "First Install" time stamp. The decoded time stamp displays in UTC time zone. Using the correct time zone offset of -5 hours, the stored time is 10/12/2022 11:17:27 AM (CDT). This matches the time stamp I

verified above from the USBSTOR Subkey. It invalidates the "First Install" time stamp reported in Figure 11. This confirms that the output reported in Figure 4 is correct, while the conflicting output reported in Figure 11 is not.

b. The 0065 subkey (**Exhibit C, Figure 14**) contains the time stamp indicating when the driver for the thumb drive was activated. The decoded time stamp again displays in UTC time zone. Using the correct time zone offset of -5 hours, the stored time is 10/12/2022 11:17:27 AM (CDT). This again matches the time stamp I verified above from the USBSTOR Subkey. And it again invalidates the time stamp reported in Figure 11. The output reported in Figure 4 again is correct, while the conflicting output reported in Figure 11 again is not.

c. The 0066 subkey (**Exhibit C, Figure 15**) contains the "Last Insertion" time stamp. The decoded time stamp again displays in UTC time zone. Using the correct time zone offset of -6 hours (the offset has changed from -5 to -6 because daylight saving time ended), the stored time is 12/20/2022 6:26:32 AM (CST). This again matches the time stamp I verified above from the USBSTOR Subkey. And it again invalidates the time stamp reported in Figure 11. The output reported in Figure 4 again is correct, while the conflicting output reported in Figure 11 again is not.

d. The 0067 subkey (**Exhibit C, Figure 16**) contains the "Last Removal" time stamp. The decoded time stamp again displays in UTC time zone. Using the correct time zone offset of -6 hours, the stored time is 12/20/2022 4:55:04 PM (CST). Again, this matches the time stamp I verified above from the USBSTOR Subkey. And it again invalidates the time stamp reported in Figure 11. The output reported in Figure 4 again is correct, while the conflicting output reported in Figure 11 again is not.

91. To recap, by using Mr. Lieb's Axiom case to manually access and decode the time stamps stored in both the USBSTOR Subkey and USB Subkey, I was able to validate the time stamps reported in Figure 4 and to invalidate the conflicting time stamps reported in Figure 11. The time stamp values in both the USBSTOR Subkey and USB Subkey for Ms. Grailer's USB

thumb drive consistently provide a "Last Insertion" date and time of 12/20/2022 at 6:26:32 AM (CST) and a "Last Removal" date and time of 12/20/2022 at 4:55.04 PM (CST).

92. Unfortunately, Mr. Lieb did not address any of the above analysis in his report. Paragraph 17 and footnote 2 of Mr. Lieb's report tell us that he relied on the Axiom outputs shown in Figure 11 as his only basis for opining that Ms. Grailer last connected her USB thumb drive to her computer on 1/8/2023 at 9:39:51 PM. (Lieb Report ¶ 17 & n.2.) But if Mr. Lieb relied on that output, he must not have manually decoded the underlying time stamp values stored in the USB Subkey. And it is very difficult to understand why not. Mr. Lieb flagged both the USBSTOR Subkey and USB Subkey outputs as "of interest" in his Axiom Case, so he must have seen that Axiom reported contradictory outputs in the information shown in Figures 4 and 11. He also must have seen that the outputs shown in Figure 11 suggested, implausibly, that Ms. Grailer first installed, last inserted, *and* last removed her USB thumb drive from the laptop all at the same time. Moreover, as depicted in Exhibits D-2 and D-5, Mr. Lieb's Axiom Case allowed him to easily access the underlying time stamp values stored in the registry subkeys simply by clicking on the hyperlinks displayed on the screen. Clicking on those hyperlinks would have allowed Mr. Lieb to access and decode the stored registry values within a matter of minutes.[10]

Windows Event Logs

93. We can also use Mr. Lieb's Axiom Case to check the results above against information separately available in the Windows event logs. As discussed above, in addition to the first and last time stamps for the activity of a USB thumb drive in the registry, the operating system created event log entries[11] for each time Ms. Grailer's USB thumb drive was connected

---

[10] During his deposition, Mr. Lieb testified that he also relied on Axiom's report, as depicted in Figure 11, that Ms. Grailer last *removed* her thumb drive from the computer at 9:39:51 PM on January 8, 2023—despite concluding that Ms. Grailer *inserted* the drive at that same second. (Lieb Dep. at pp. 254, 284–285.) It should go without saying that this is not reasonable. Aside from the outputs in Figure 11 being invalidated by the underlying time stamps, inserting and removing the thumb drive at the same second would have left Ms. Grailer with no time to engage in the copying activities that Mr. Lieb alleges. This is another instance of Mr. Lieb failing even to tell a story that makes sense.

[11] These event log entries have an Event ID of 1006 and are stored in a specific event log: Microsoft-Windows-Partition%4Diagnostic.evtx. These events are created when a USB thumb drive is connected and detected as disconnected.

and disconnected. Those entries were extracted by Axiom into Mr. Lieb's Axiom Case, but Mr. Lieb did not discuss them in his report or declarations. The event log entries are critical for two reasons: (i) They show the connection history of the USB thumb drive; and (ii) they allow us to test the time stamps stored in the registry's USBSTOR Subkey and USB Subkey.

94. Using Mr. Lieb's Axiom Case, the relevant Windows event log events can be found simply by searching for the Emtec thumb drive's internal USB serial number (iSerialNumber 070B4A71ADB22353). **Exhibit C, Figure 17** contains a depiction of all event log entries related to the Emtec USB thumb drive, in chronological order for Event ID 1006 from the Grailer Image. The serial number outlined in yellow confirms we are still looking at the correct device. For reference, a full-page screenshot from Axiom including the depiction used in Figure 17 is also attached hereto as **Exhibit D-6**. Exhibit D-6 includes all 34 storage device entries (Event ID 1006) for the Grailer Image, including entries for two devices that were connected on February 8, 2023.[12]

95. Figure 17 shows the dates and times of connection and disconnection. Ms. Grailer's Emtec USB thumb drive was first connected to the computer no later than March 16, 2022. The last eight entries in Figure 17, which show four connections and disconnections, were from October 12, 2022 through December 20, 2022. The last two entries show that the USB thumb drive was last connected and disconnected on December 20, 2022. Those time stamps match the "Last Insertion" and "Last Removal" time stamps that, above, I was able to access and decode from both the USBSTOR Subkey and USB Subkey. Figure 17 shows no events for the Emtec USB thumb drive after December 20, 2022. As depicted in Exhibit D-6, after December 20, 2022, no USB storage device was connected to the laptop until February 8, 2023, the day Mr. Lieb imaged the laptop.

---

[12] Each event log entry for Event ID 1006 also lists the "disk" serial number of the storage device. On some USB storage devices, the disk serial number may be different than the internal USB serial number (iSerialNumber). The disk serial number for the Emtec USB Drive is 027305B340A0, as shown in Exhibit D-6. The iSerialNumber, 070B4A71ADB22353, appears as a suffix to the ParentID in Exhibit D-6. It is important to note that the Emtec USB drive has two different serial numbers, because information displayed for the same device may simply refer to a "serial number."

96. Thus, the time stamps in the Windows event logs match—and validate—the time stamp values stored in the USBSTOR Subkey and USB Subkey. So, we now have three separate information sources telling us that Ms. Grailer's USB thumb drive was last connected to the computer on December 20, 2022, and that the computer last detected the thumb drive's removal on December 20, 2022 at 4:55:04 PM (CST).

97. Mr. Lieb's omission of the event log data depicted in Figure 17 and Exhibit D-6 is very problematic. Mr. Lieb testified during his deposition that he knows that Windows event logs record each time a USB thumb drive is connected and disconnected. (Lieb Dep. at pp. 213–214.) As shown in Figure 17 and Exhibit D-6, the Windows event logs available to Mr. Lieb in his Axiom Case clearly showed that Ms. Grailer did not connect her thumb drive to the computer after December 20, 2022. An objective and experienced examiner in Mr. Lieb's position would have acknowledged that the Windows event logs showed no events for Ms. Grailer's thumb drive after December 20, 2022, and would have explained the basis (if there could be any) for disregarding that evidence. Mr. Lieb, however, simply omitted the event logs from his report, as well as from his earlier declarations.

98. Before I move on, I note that the event log data in Figure 17 and Exhibit D-6 demonstrates that the "First Install" time stamps stored in both the USBSTOR Subkey and the USB Subkey can be misleading if not interpreted with care. The USBSTOR Subkey and USB Subkey both provided a "First Install" time stamp of 10/12/2022 11:17:28 AM (CDT). However, the event log data in Figure 17 and Exhibit D-6 show that Ms. Grailer had her USB thumb drive connected no later than March 16, 2022. This discrepancy is not surprising. The Windows operating system will sometimes clean up old information on previously connected USB devices and will remove information from the registry. If that occurs, it will be noted in one of the archived setupapi.dev logs. Then, the next time the same USB device is inserted into the computer, the registry information will be added again and a new "first" install time stamp will appear. This is another example of why an examiner must not blindly rely on each output that Axiom extracts from a computer's image, but instead must check each output against other available information.

Windows Registry – MountPoints2 Subkey

99. There is one other place I can use Mr. Lieb's Axiom Case to look at in order to check the results above. As discussed above, the Windows registry includes another subkey called the "MountPoint2 Subkey." That subkey provides another reference of when a USB storage device was last connected to the computer. The MountPoints2 Subkey[13] is associated with the user account that plugged in the USB storage device and contains further subkeys for each USB storage device that was connected. **Exhibit C, Figure 18** is a depiction of the MountPoints2 Subkey in the profile hive for Ms. Grailer's account from the Grailer Image.

100. The subkey for each mounted storage device is represented with a volume GUID ("Volume GUID Subkey"). The Volume GUID Subkey for Ms. Grailer's Emtec USB thumb drive is {bc60243f-0db6-11eb-a291-3024321d29bd}.[14] I have outlined that Volume GUID Subkey in red in Figure 18.

101. Each time a USB thumb drive is connected to the computer, it is mounted and assigned a drive letter, such as drive D. At that time, the Volume GUID Subkey is updated, which updates the "last written" time of the subkey. This "last written" time for a device's Volume GUID Subkey in the MountPoints2 Subkey can be used as another reference for last time the device was connected to the computer.

102. As shown in **Exhibit C, Figure 19**, Mr. Lieb's Axiom Case shows the last written time of the Volume GUID Subkey for Ms. Grailer's USB thumb drive as 12/20/2022 6:26:42 AM (CST). This is the time stamp that Axiom uses for "Last Connected Date/Time" shown in Figure 4, where Axiom also reported time stamps from the USBSTOR Subkey (as discussed above). This time stamp is 10 seconds later than the "Last Insertion" time stamp (12/20/2022 6:26:32 AM CST) that we obtained and validated earlier from both the USBSTOR Subkey and USB Subkey.

---

[13] Located in the user profile hive at SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2

[14] The volume GUID is related to the System hive in the MountedDevices subkey which stores a matching volume GUID (\??\Volume{bc60243f-0db6-11eb-a291-3024321d29bd}). The value data contains the vendor name, product name, revision number, and USB serial number similar to Figure 1.

That difference is expected and is attributable to the delay between when the USB thumb drive was plugged in to the computer and when Windows "mounted" the device and assigned it a drive letter.

103. The MountPoints2 Subkey thus further validates the December 20, 2022 time stamps I obtained above from the USBSTOR Subkey, USB Subkey, and Windows event logs. So, altogether, we now have four separate information sources telling us that Ms. Grailer's USB thumb drive was last connected to the computer on December 20, 2022. If Ms. Grailer had connected the Emtec USB thumb drive to her laptop after December 20, 2022, the last written time of the device's Volume GUID Subkey would have been updated, just as the Windows event logs and the other time stamps reviewed above would have been updated. But that did not occur.

104. Mr. Lieb does not discuss the MountPoint2 Subkey in his report. He cited the MountPoints2 Subkey in his first declaration, so he must have reviewed it at some point. (Lieb Decl. ¶ 26 and n.5, Feb. 21, 2023.) But Mr. Lieb omits any discussion of the MountPoints2 Subkey in his report. During his deposition, Mr. Lieb testified that he was "not familiar with" the MountPoints2 Subkey. (Lieb Dep. at pp. 212–213.) That is odd given that Mr. Lieb cited the MountPoints2 Subkey in his February 2023 declaration.

105. We have now finished examining the information available in Mr. Lieb's Axiom Case relating to when Ms. Grailer last had her USB thumb drive connected to her laptop. To recap, all that information led to the same answer: December 20, 2022. If Ms. Grailer had connected her USB thumb drive to her laptop after December 20, 2022, several things would have happened in the computer: (i) the "Last Insertion" and "Last Removal" time stamps in the 0066 and 0067 subkeys in the USBSTOR Subkey would have updated; (ii) the corresponding "Last Insertion" and "Last Removal" time stamps in the 0066 and 0067 subkeys in the USB Subkey would have updated; (iii) the Windows event logs shown in Exhibit D-6 would have recorded a connection and disconnection sometime between December 20, 2022 and February 8, 2023; and (iv) the last written time of the Volume GUID Subkey for Ms. Grailer's USB thumb drive also would have updated. Ms. Grailer could not have used her USB thumb drive on the laptop after December 20, 2022 without causing updates in all those different locations in the computer. None

of the updates occurred, so we know the USB thumb drive could not have been connected after December 20, 2022. This also matches what we saw in the Digital Guardian report, which demonstrates that Ms. Grailer last copied files to her USB thumb drive on December 20, 2022.

5. USING OTHER SOFTWARE FOR VALIDATION

106. As mentioned above, a forensic examiner may also use other forensic software to validate the results provided by the first software used. According to one of his invoices, Mr. Lieb used a second software tool called OSForensics to generate an "OSForensics forensic database [*i.e.,* case] of Jessica Grailer Ecolab laptop" on February 13, 2023. (ECOLAB 021856.) I did not receive a copy of Mr. Lieb's OSForenics case, but I independently used OSForensics (version 10.0.1016) to further review information about Ms. Grailer's Emtec USB thumb drive in the Grailer Image. Any other person with access to the Grailer Image could do the same, just as Mr. Lieb used OSForensics to generate his own OSForensics case from the Grailer Image (but without providing his OSForensics case for me to review).

107. OSForensics lists information about Ms. Grailer's Emtec USB thumb drive in a category that OSForensics calls "USB Devices." A full-page screenshot of OSForensics' depiction of that information is attached hereto as **Exhibit D-7**. Exhibit D-7 references Ms. Grailer's Emtec USB thumb drive in three entries. For ease of reading, I have attached an excerpt showing only those three entries at **Exhibit C, Figure 20**.

108. The three entries shown in Figure 20 depict information that OSForensic extracted from (i) the USB Subkey, (ii) the USBSTOR Subkey, and (iii) the device's last entry in the Windows event logs. I note that the first two entries use the device's iSerialNumber of 070B4A71ADB22353, while the final entry uses its disk serial number of 027305B340A0.

109. The entries in Figure 20 match the time stamps that, above, I obtained and validated using Mr. Lieb's Axiom Case. In Figure 20, OSForensics reports that, according both USBSTOR Subkey and the USB Subkey, Ms. Grailer's USB thumb drive was last connected to the computer at 12/20/2022 6:26:32 AM (CST). It also reports that, according to the Windows event logs, the last event involving the USB thumb drive (which would have been a disconnection

event) occurred at 12/20/2022 4:55:04 PM (CST). These are the same dates and times that I found by examining the same information sources through Mr. Lieb's Axiom Case.

110. OSForensics also extracts Event ID 1006 entries that I described above from the Windows event logs.[15] Those entries are listed in OSForensics' "USB History" category. A full-page screenshot of OSForensics' depiction of that information is attached hereto as **Exhibit D-8**. The last two entries for Ms. Grailer's USB thumb drive both were on December 20, 2022. For ease of reading, I have attached an excerpt of only those two entries at **Exhibit C, Figure 21**.

111. The event log entries depicted in Exhibit D-8 and Figure 21 again match the event log entries that Axiom extracted into Mr. Lieb's Axiom Case. (Compare Exhibit D-6 with Exhibit D-8.) This is yet more validation that December 20, 2022 is in fact when Ms. Grailer last had her USB thumb drive connected to her laptop.

112. The event log entries depicted in Exhibit D-8 (Events 129 and 130) are also listed in yet another category in OSForensics called "Event Logs, Storage Device Usage." A depiction of that information is attached hereto as **Exhibit D-9**. There, again, we see that the event logs for Ms. Grailer's USB thumb drive ended on December 20, 2022.

113. To recap, the information extracted and displayed by OSForensics uniformly confirms that Ms. Grailer's USB thumb drive was last connected to her laptop on December 20, 2022. Although Mr. Lieb had this information available to him in the OSForensics case he created, he did not discuss any of it in his report. As noted above, Mr. Lieb testified during his deposition that it is "not a good idea" to rely on only one software tool such as Axiom when the examiner has a second tool such as OSForensics available. (Lieb Dep. at p. 219.) Nonetheless, Mr. Lieb omitted any discussion of OSForensics' outputs in his report, as well as in his earlier declarations, when addressing when Ms. Grailer last had her thumb drive connected to the computer.

[15] Microsoft-Windows-Partition%4Diagnostic.evtx

6. WHY DID FIGURE 11 REPORT INCORRECTLY IN AXIOM?

114. We've done more than enough to demonstrate that the outputs reported by Axiom in Figure 11 were incorrect. Those outputs were internally inconsistent—because Ms. Grailer could not have first installed, last inserted, *and* last removed her thumb drive all at the same second—and were also invalidated by the USB Subkey's "Last Insertion" and "Last Removal" time stamps that Figure 11 was supposed to be reporting. They were further invalidated by the additional time stamps stored in the USBSTOR Subkey, the Windows event logs, and the MountPoints2 Subkey, as discussed above. And, when we examined the same information using OSForensics—including the information that OSForensics reported from the USB Subkey—we found that OSForensics reported the correct (December 20, 2022) outputs without any error. Still, one might ask the question: *Why was Figure 11 wrong?* And that is a question that I also asked, and endeavored to answer. Although Mr. Lieb omitted from his report all the many time stamps that did not fit his conclusion, an experienced and objective examiner would work to understand and to explain outlier data such as we saw above in Figure 11. I did that when performing my analysis.

115. Most of the errors shown in Figure 11 are attributable to a bug in the Axiom software. In fact, they are attributable to a bug that I reported to Magnet Forensics, the developer of Axiom, and which Magnet Forensics has fixed since Mr. Lieb generated his Axiom Case in February 2023.

116. My bug report to Magnet Forensics initially started as bug report H-00083904 and was escalated to the development team for correction (tracked internally as "CARS-508").

117. In August 2023, Magnet Forensics released Axiom version 7.4. The release notes for Axiom version 7.4 are attached hereto as **Exhibit D-10**. The "Bug Fix" section on page 4 refers to my bug report: "*Some timestamps for USB Devices were being reported incorrectly. - CARS-508.*"

118. I recently used Axiom version 7.8 to extract from the Grailer Image the same information that is shown in Figure 11. A screenshot of that recent extraction is attached hereto as

Exhibit D-11. The "ARTIFACT INFORMATION" corresponding to Figure 11 appears in the upper part of Exhibit D-11's right-hand column.

119. As depicted in Exhibit D-11, after responding to my bug report in August 2023, Axiom now correctly reports the "Last Insertion" and "Last Removal" time stamps from the USB Subkey. Specifically, consistent with the other information I examined above, Axiom now reports a "Last Insertion" time stamp of 12/20/2022 6:26:32 AM and a "Last Removal" time stamp of 12/20/2022 4:55:04 PM. As shown in Exhibit D-11, Axiom no longer reports the incorrect "Last Insertion" and "Last Removal" time stamps that we saw in Figure 11.

120. We still, however, have one last outlier time stamp left to explain. Even now, in Exhibit D-11, Axiom reports a "Last Connected" time stamp of 1/8/2023 9:39:51 PM (CST). That "Last Connected" time stamp conflicts with the "Last Connected" time stamp of 12/20/2022 6:26:42 AM (CST) that Axiom reported for the same device in Exhibit D-2 and Figure 4, as well as with the "Last Insertion" time stamp of 12/20/2022 6:26:32 AM that Axiom reports in Exhibit D-11 itself (and with the other time stamps that we reviewed above). But the 1/8/2023 9:39:51 PM (CST) "Last Connected" time stamp persists in Exhibit D-11, and we should understand why it cannot be relied upon.

121. The reason Axiom continues to report two different "Last Connected" time stamps for the same device is that Axiom uses two different information sources to report those time stamps. In Exhibit D-2 and Figure 4, Axiom reports the thumb drive's "Last Connected Date/Time" as the last written time of the Volume GUID Subkey, as noted in paragraph 102 above. In Exhibit D-11, however, Axiom instead uses the last written time of the "Device Subkey" for the Emtec USB Drive (VID_6557&PID_4200) in the USB Subkey.[16] That latter time stamp—the last written time of the thumb drive's "Device Subkey" in the USB Subkey—is the specific time stamp that Mr. Lieb cites in footnote 2 of his report as his only support for his claim that Ms. Grailer connected her thumb drive to the computer at 9:39:51 PM on January 8, 2023.

[16] The Device Subkey (VID_6557&PID_4200) for Ms. Grailer's Emtec USB Drive in the USB Subkey is outlined in green in Exhibit C, Figure 2.

(Lieb Report ¶ 17 n.2.) Generally, all the various time stamps for a single device, including the last written time of a device's "device subkey" in the USB subkey, will be consistent with one another, and there will be no discrepancies for the examiner to consider and resolve. But sometimes, as here, they do not. Here, although Axiom correctly reports the last written time of the thumb drive's "Device Subkey" in the USB Subkey, that "last written" time stamp does not accurately reflect when Ms. Grailer last connected her thumb drive to the computer.

122. We can see that this time stamp is unreliable as a reference for actual connection activity, not just by comparing it to the conflicting time stamps that we reviewed above, but also by examining all the *other* time stamps that updated in the USB Subkey at the exact same time of 9:39:51 PM on January 8, 2023. That examination shows that the last written time of the thumb drive's "Device Subkey" in the USB Subkey updated at 9:39:51 PM on January 8—not because the thumb drive was connected—but rather as part of a mass changes that affected hundreds of "last written" time stamps in the USB Subkey all at the same second.

123. The Windows registry stores a "last written" time stamp for every subkey. Typically, when a value stored within a given subkey is added or updated, the registry will update the last written time stamp of that subkey. However, the operating system may also update all of the last written time stamps within a subkey even when the values within those subkeys have *not* changed. This type of update occurred on the Grailer Laptop on January 8, 2023 at 9:39:51 PM (CST), as explained below.

124. As depicted in **Exhibit C, Figure 22**, the "Device Subkey" for the Emtec USB Drive (VID_6557&PID_4200) in the USB Subkey shows a "last written" time of January 8, 2023 at 9:39:51 PM (CST). Again, Axiom used this time stamp to populate the Last Connected Date/Time in Exhibit D-11. But Figure 22 does not does not depict the "last written" time stamps of other surrounding registry subkeys. The examiner thus must look at the surrounding time stamps of the entire USB Subkey, to see if other subkeys show identical "last written" time stamps. In this case, the examiner will find that more than 700 "last written" time stamps in the USB Subkey all updated to the exact same date and time of January 8, 2023 at 9:39:51 PM (CST).

125. **Exhibit C, Figure 23** depicts 19 of the 21 subkeys in the USB Subkey all having the same "last written" time stamp of January 8, 2023 at 9:39:51 PM. The only two subkeys that do not have that time stamp are outlined in red. Those two subkeys are dated February 8, 2023, the day that Mr. Lieb imaged the Grailer Laptop. They were added prior to the computer being imaged on 2/8/2023 at 4:37:20 PM (CST). They were added to the registry because Mr. Lieb or his company connected two USB devices (Kingston thumb drive and a Samsung external USB drive) to the computer prior to imaging. All 19 subkeys that existed before Mr. Lieb or his company added two new subkeys on February 8, 2023 have the same "last written" time stamp of 9:39:51 PM on January 8, 2023.

126. A listing of those 19 subkeys stored in \ControlSet001\Enum\USB as well as all the further subkeys within the 19 subkeys shows a total of 713 subkeys with exactly the same "last written" time of January 8, 2023 at 9:39:51 PM. This list is attached hereto as **Exhibit D-12**.

127. The 713 subkeys listed in Exhibit D-12 include the 0064 subkey (First Install), 0065 subkey (Install), 0066 subkey (Last Insertion), and 0067 subkey (Last Removal) in the USB Subkey for Ms. Grailer's USB thumb drive. They also include 41 other subkeys for the same device (all these entries are highlighted in yellow), as well as hundreds of other subkeys that have nothing to do with Ms. Grailer's USB thumb drive. They do not, however, include any of the subkeys in the USBSTOR Subkey for Ms. Grailer's USB thumb drive. The mass changes reflected in Exhibit D-12 occurred exclusively within the USB Subkey. In my experience, this massive update of last written time stamps for all subkeys is not a common occurrence. But it does occur, and it clearly occurred here based on what is shown in Exhibit D-12.

128. We know the mass changes reflected in Exhibit D-12 were not caused by Ms. Grailer connecting her USB thumb drive to the computer. If Ms. Grailer had connected her thumb drive, the changes shown in Exhibit D-12 would be both overinclusive and underinclusive. They would be overinclusive because connecting Ms. Grailer's USB thumb drive would not have caused an update to the "last written" time stamp of *every* subkey in the USB Subkey for that device, let alone to hundreds of other subkeys in the USB Subkey that are unrelated to Ms. Grailer's USB thumb drive. And they would be underinclusive because connecting the USB

thumb drive would have caused updates to (i) the "Last Insertion" time stamp stored in the 0066 subkey in the USB Subkey; (ii) the corresponding "Last Insertion" time stamp stored in the 0066 subkey in the USBSTOR Subkey; (iii) the Windows event logs; (iv) the "last written" time of the Volume GUID Subkey for Ms. Grailer's USB thumb drive. But as demonstrated above, none of those updates occurred.

129. Exhibit D-12 illustrates why an examiner should not simply assume that the "last written" time stamp for a subkey accurately reflects the time that a USB thumb drive was connected or disconnected. Together with Figure 11 and Exhibit D-11, as well as Magnet Forensics' response to my bug report, Exhibit D-12 also illustrates what Magnet Forensics says in the materials in Exhibit D-1: "Timestamps for USB devices are retrieved from the device registry, and due to the behavior of registry keys, may not always accurately reflect the true time when a user performed a certain action. . . . For this reason, it's important to verify these timestamps with other USB-related artifacts, such as . . . other timestamp data on the computer where the USB device was plugged in."

C. LIEB'S OTHER CITED EVIDENCE REGARDING JANUARY 8, 2023

130. Mr. Lieb cites two pieces of evidence to support his expressed opinion that Ms. Grailer copied various files and folders to her USB thumb drive on January 8, 2023. First, he cites what is known as the Update Sequence Number (USN) change journal (file name = $UsnJrnl:$J) in the Grailer Image. He cites the USN change journal as the only evidence to support his claim that Ms. Grailer used her USB thumb drive on January 8, 2023 to copy the files that Mr. Lieb lists in Exhibit E to his report. (Lieb Report ¶ 18 & n.3.) Second, Mr. Lieb cites Exhibit F to his own report. Mr. Lieb's Exhibit F contains screenshots that he prepared with OSForeniscs software, showing "Master File Table (MFT) Modified" time stamps for different folders and files in the Grailer Image. Mr. Lieb cites his Exhibit F to support his expressed opinion that "Jessica Grailer copied these files and folders [listed in Mr. Lieb's Exhibit F] to the Emtec Drive on January 8, 2023, in addition to the files described in [Mr. Lieb's] Exhibit E." (Lieb Report ¶ 19.)

131. In relying on this evidence to support his claim of copying, Mr. Lieb makes an assumption that an experienced and objective examiner would recognize as unsound. The USN

change journal and MFT Modified dates shown in Mr. Lieb's Exhibit F both reflect mass activity involving large numbers of files or folders at the same or nearly the same time. In his report, Mr. Lieb assumes that such mass activity could only be explained by Ms. Grailer's copying the files and folders to her USB thumb drive. (Lieb Report ¶¶ 18–19.) That assumption is not reasonable.

132. As we will see below, much of the evidence Mr. Lieb cites is not even consistent with a user's copying files or folders to a USB thumb drive. This is because Mr. Lieb relies on evidence of activity that occurred simultaneously to files spread across multiple different folders, which in many cases a user could not plausibly have targeted all at the same time.

133. In any event, even to the extent the evidence Mr. Lieb cites might be *consistent* with copying, an experienced and objective examiner would recognize that mass changes in the USN change journal and to folders' MFT Modified dates also may occur due to programs and services running in the background. Accordingly, such mass changes are not on their own persuasive evidence of copying. Rather than leaping to a conclusion that copying is indicated, an experienced and objective examiner would attempt to corroborate and validate that hypothesis by examining the sort of evidence that I covered in the sections above.

134. We have already seen that the evidence covered above, rather than corroborating Mr. Lieb's claim, rules out the hypothesis that Ms. Grailer copied files (or folders of files) to her USB thumb drive on January 8. Most importantly, if Ms. Grailer had copied files (or entire folders of files) to an external storage device as Mr. Lieb claims, we would expect to see many entries in the Digital Guardian report recording that activity. Instead, as discussed above, the Digital Guardian report shows the opposite. In addition, if Mr. Lieb were right in claiming that Ms. Grailer copied files to her Emtec USB thumb drive on January 8, 2023, we would expect to see January 8, 2023 updates to (i) the "Last Insertion" time stamp stored in the 0066 subkey in the USB Subkey for Ms. Grailer's thumb drive; (ii) the corresponding "Last Insertion" time stamp stored in the 0066 subkey in the USBSTOR Subkey for the thumb drive; (iii) the Windows event logs relating to the thumb drive; and (iv) the "last written" time of the Volume GUID Subkey for the thumb drive. But as demonstrated above, none of those updates occurred, as confirmed with Mr. Lieb's Axiom Case and by doublechecking those results with the competing OSForensics

software tool. Also, if Ms. Grailer had copied files to her thumb drive, she would have had to do that *after* connecting the thumb drive to the computer. But as noted above and again below, the USN change journal activity and MFT Modified Dates that Mr. Lieb points to came *before* the 9:39:51 PM (CST) time at which he claims Ms. Grailer connected her thumb drive on January 8, 2023.

135. Nonetheless, I will go on below to address the evidence Mr. Lieb cites, as well as the kinds of activities that may result in it. I will first address the USN change journal. Then I will turn to the MFT Modified dates.

1. USN CHANGE JOURNAL

136. The USN change journal is a component of the Windows New Technology File System (NTFS) that provides a log of changes made to files. For example, as files and directories are created, deleted, and modified, the file system creates records in the USN change journal. Each record includes basic information about the type of change that occurred.

137. The record structure of the USN change journal has a field called "Reason." This field contains a 4-byte hex value that provides a "reason" for the event. This field is populated in the USN change journal entries in Mr. Lieb's Axiom Case.

138. All of the reasons that are defined by Microsoft for version 2 of the USN change journal are attached hereto as **Exhibit D-13**.[17] None of those reasons corresponds to copying a file to an external storage device. This is because, unlike endpoint programs such as Digital Guardian, the USN change journal is not intended to track activities such as user copying.

139. In the Grailer Image, the USN change journal contains a total of 360,086 entries, which begin on 1/8/2023 at 7:20:27 PM (CST). There are no entries prior to that time. The last entry is on 2/8/2023 at 4:37:50 PM (CST). The journal contains a total of 118,294 entries on February 8, 2023, starting on 2/8/2023 at 11:44:12 AM (CST). Those 118,294 entries occurred after Mr. Lieb took custody of the computer, before he imaged it.

[17] https://learn.microsoft.com/en-us/windows/win32/api/winioctl/ns-winioctl-usn_record_v2

140. The entries created on February 8, 2023 resulted in the deletion of earlier entries that would have existed on the computer when Mr. Lieb took custody of it. The USN change journal is designed to function as a temporary, not permanent, record to assist in Windows' operations. The maximum size of the USN change journal on Ms. Grailer's laptop was set to 32 megabytes. The change journal will get truncated[18] as new entries are added. Thus, the 118,294 entries created on February 8, 2023 would have resulted in the removal of change journal entries from prior to 1/8/2023 at 7:20:27 PM (CST).

141. Mr. Lieb listed nothing except file names in his Exhibit E. He omitted from the exhibit (and his report) any of the specific times when he claims that Ms. Grailer copied each listed file. He also failed to include any USN change journal "reasons"—or any other information from the USN change journal. In footnote 3 of his report, Mr. Lieb cites to the USN change journal in its entirety. He did not do what an experienced and objective examiner would have done, which is to identify the specific entries of interest in the USN change journal, and to construct an evidence-based timeline showing exactly when Ms. Grailer allegedly connected her USB thumb drive to her laptop on January 8, 2023; when she allegedly copied each specific file or folder of files to her thumb drive while it was connected; and when she allegedly disconnected the thumb drive after that alleged copying.

142. Before I go on to discuss Mr. Lieb's Exhibit E in more detail, I note two preliminary but significant problems with the exhibit. First, I was unable to find USN change journal entries relating to 72 of the 259 files listed in Mr. Lieb's Exhibit E. Those files are listed in **Exhibit D-14**, attached hereto. I do not know what evidence, if any, Mr. Lieb claims supports his conclusion that these 72 files were "exfiltrated." The only evidence Mr. Lieb cited was the (entire) USN change journal, but that is no help for files that have no entries in that journal.

143. Second, with respect to the files for which I did find USN change journal entries, most of those journal entries pre-date the time (9:39:51 PM (CST) on January 8, 2023) when Mr.

[18] https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/fsutil-usn

Lieb claims Ms. Grailer connected her thumb drive to the computer. This takes us back to the problem I addressed above. According to footnote 3 in his report, Mr. Lieb's evidence that files were copied supposedly consist of USN change journal entries that Mr. Lieb does not specify, but which appear mostly to have occurred before 9:39:51 PM (CST) on January 8, 2023. That cannot be reconciled with (i) the fact that 9:39:51 PM is the only time when Mr. Lieb claims that Ms. Grailer connected her thumb drive on January 8, 2023 (and Ms. Grailer could not have copied files to her thumb drive *before* connecting it); and (ii) Mr. Lieb's testimony during his deposition that Grailer did not begin "exfiltrating" files until she allegedly connected her thumb drive at 9:39:51 PM on January 8, 2023.

144. Without addressing every single file listed in Mr. Lieb's Exhibit E, I nonetheless conducted the analyses set forth below to confirm that entries in the USN change journal provide no basis for Mr. Lieb's assumption that "copying" must be the explanation. Below, I begin with the first 79 files listed in in Mr. Lieb's Exhibit E, all of which Mr. Lieb tagged in his Axiom Case. Then I analyze data relating to Excel spreadsheet files in the Grailer Image. Finally, I address the last 23 files listed in Mr. Lieb's Exhibit E, all of which were attached to emails that Ms. Grailer either received or sent on January 8, 2023.

The First 79 Files in Lieb's Exhibit E

145. In reviewing Mr. Lieb's Axiom Case, I found that he tagged the first 79 files from his Exhibit E as "EXFILTRATED 1/8/2023" in the USN change journal section. I extracted information associated with those 79 files from Mr. Lieb's Axiom Case. I have depicted that information in **Exhibit D-15**, attached hereto. I've highlighted several entries in Exhibit D-15, for reasons I will explain below. Exhibit D-15 contains the file name, the USN change journal number, the time stamp (in CST) of the change entry, the reason, the master file table (MFT) record number for the file, the MFT parent record of the file,[19] and the Item ID in the Axiom Case.

[19] Each file is located in a folder, which is considered the "parent" of the file. The MFT parent record number can be cross-referenced to the MFT to determine the exact folder name and path.

146. The time stamps for each file listed in Exhibit D-15 occurred within two seconds, between 1/8/2023 7:20:38 PM and 1/8/2023 7:20:39 PM (CST). I agree that a user cannot open 79 files in two seconds. However, this does not mean the inference should be that the 79 files must have been copied to a USB thumb drive, especially a thumb drive that was not even connected to the computer at 1/8/2023 7:20:38 PM (CST).

147. Even setting aside that the activity shown in Exhibit D-15 preceded the time when Mr. Lieb claims Ms. Grailer connected her USB thumb drive, an experienced and objective examiner would consider whether other activity on the computer, including programs and services running in the background, can explain the USN change journal entries. When the Grailer Laptop starts up, there are over 135 kernel and file system drivers that are started by the Windows operating system. There are over 90 additional services (programs) that are started immediately[20] following that process. Additional programs are set to start based on their settings, such as the computer starting up or a user logging in. All this information was extracted by Axiom and listed in the System Services and Startup Items categories. These services and programs are active in the background while the computer is running and can impact file creation, modification, and deletion. In turn, this will affect date and time stamps on the computer, as demonstrated below.

148. By examining the Windows event logs, I found logs entries that were created 8 seconds before the two seconds of activity shown in Exhibit D-15. These log entries show the computer was successfully logged into using the "jlgrailer" account on 1/8/23 at 7:20:30 PM (CST). This event is depicted in a full-page screenshot of Axiom attached hereto as **Exhibit D-16**. This occurred after the computer was locked at 7:16 PM, as depicted in **Exhibit C, Figure 24**, which would have occurred due to 15 minutes of inactivity.[21] Therefore, the rapid file activity shown in Exhibit D-15 occurred 8 seconds after the login and screen unlock.

---

[20] Windows starts these services automatically, which is reflected as the "start type" of the service.
[21] The computer policy was set to lock the computer after 15 minutes of inactivity (Software hive, Microsoft\Windows\CurrentVersion\Policies\System\InactivityTimeoutSecs).

149. I analyzed the time period starting at 1/8/2023 7:20:30 (CST) and found that the change journal entries for the 79 files in Exhibit D-15 were all related to programs running in the background:

a. Two files listed in Mr. Lieb's Exhibit E and my Exhibit D-15 are "event-id-524505424.mark" and "event-id-524505793.mark." For reference, these two files are highlighted in Exhibit D-15. They were located in the following parent folder (Parent MFT Record 39415): Program Files\Endgame. The reason listed for these files' entries in the USN change journal is that the files were being renamed. These files are related to an installed program/service running in the background called "Endpoint Sensor."[22] By searching the USN change journal for files that matched the same file naming convention, I found a total of 2,424 entries. This file activity occurred on 1/8/2023 between 7:20:38 PM and 10:02:27 PM (CST) and on 2/8/2023 between 11:44:12 AM and 4:27:25 PM (CST). On 2/8/2023, the computer was in Mr. Lieb's custody. The USN change journal entries relating to these files obviously had nothing to do with copying.

b. Two other files listed in Mr. Lieb's Exhibit E and my Exhibit D-15 are "C8F375B2-E5B9-4AA0-BEFF-954B39945490qwerty.bak" and "B62E4989-07E9-4DD7-A64C-260FD8B14D08qwerty.bak." For reference, these two files are also highlighted in Exhibit D-15. They were located in the following parent folder (Parent MFT Record 59390): \Users\JLGRAILER\AppData\Roaming\09D849B6-32D3-4a40-85EE-6B84BA29E35B\msgs. The reason listed for these files in the USN change journal is that the files were created and deleted. These files are related to the Digital Guardian program/service[23] running in the background. By searching the USN change journal for files that matched the same file naming convention, I found a total of 728 entries. This file activity occurred on 1/8/2023 between 7:20:38 PM and 9:56:26 PM (CST), and on 2/8/2023 between 11:44:22 AM and 4:36:17 PM (CST). On

---

[22] This computer has programs and services that are configured to start when the computer is powered on. Axiom displays this information in a section called System Services.

[23] Axiom displays this service information in a section called System Services.

2/8/2023, the computer was in Mr. Lieb's custody. Again, the USN change journal entries relating to these files obviously had nothing to do with copying.

c. Two other files listed in Mr. Lieb's Exhibit E and my Exhibit D-15 are "_c19b1176-a415-4ba1-997d-c5536d9c62c0.zip" and "_7391f34f-0fa1-441e-a523-3789cd47bdbd.json." For reference, these two files are also highlighted in Exhibit D-15. They were located in the following parent folder (Parent MFT Record 471055): \Users\JLGRAILER\AppData\Local\Temp. The reason listed for these files in the USN change journal is that the files were being deleted. Since these are temporary files and have been deleted, I have been unable to determine what program/service created these files. However, I can tell by searching the USN change journal that files matching the same file naming convention were being created and deleted every 20 minutes (*i.e*, 7:20 PM, 7:40 PM, 8:00 PM, 8:20 PM, etc) in the user's Temp folder. This file activity occurred on 1/8/2023 between 7:20:28 PM and 10:00:35 PM (CST). Again, the USN change journal entries relating to these (temporary) files obviously had nothing to do with copying.

d. One other file listed in Mr. Lieb's Exhibit E and my Exhibit D-15 is "Host-Diagnostics.log." For reference, this file is also highlighted in Exhibit D-15. It was located in the following parent folder (Parent MFT Record 188486): \Users\JLGRAILER\AppData\Roaming\Ecolab\CWO\Logs. Similar to the file activity above, I found that this log file was being written in the same 20 minute increment. By searching the USN change journal for this file name, I found a total of 102,320 entries. This file activity occurred on 1/8/2023 between 7:20:27 PM and 10:00:35 PM (CST). Again, the USN change journal entries relating to this file obviously had nothing to do with copying.

150. The remaining 72 files listed in Mr. Lieb's Exhibit E and my Exhibit D-15 are located in the same parent folder (Parent MFT Record 348084): \Users\JLGRAILER\OneDrive - Ecolab\Desktop. This is a folder managed by the OneDrive service. Microsoft OneDrive[24] was

[24] Microsoft OneDrive is a cloud-based file storage program that is designed to automatically keep files and folders stored on the computer in sync with files and folders stored on the cloud server.

actively working in the background during the time after the login and screen unlock at 1/8/2023 7:20:30 (CST). This is reflected in the OneDrive sync logs.[25] By reviewing the OneDrive sync logs and looking at the USN change journal, I found that after the login and screen unlock, OneDrive began synchronizing files that it was managing on the computer. At the conclusion of that synchronization process, OneDrive wrote data to a log called SyncDiagnostics.log[26] at 1/8/2023 7:21:53 PM (CST). This log file is refreshed with new information at the conclusion of each synchronization process. OneDrive's synchronizing activities would have resulted in USN change journal entries for the synchronized files, and those activities most likely explain the entries for the 72 remaining files listed in Mr. Lieb's Exhibit E and my Exhibit D-15.

151. All this illustrates why an experienced and objective examiner would not simply assume that mass USN change journal entries indicate copying by the user. While the USN change journal can provide some insight into file activity on the hard drive, it does not provide detailed information such as whether files were copied to an external storage media, and it is not designed to serve that purpose. This is why the use of a third-party endpoint program like Digital Guardian is important; it provides a detailed event log, not provided by the operating system, pertaining to events where a user actually copies files to external storage media.

Excel Files in the Grailer Image

152. I also examined Excel files in the Grailer Image, since many of the files listed in Mr. Lieb's Exhibit E are Excel spreadsheets. Forensic software such as Axiom can organize files into different categories, like file types such as Excel files. Those categories can then be filtered or sorted, such as by date and time. I used Axiom to do this in the Grailer Image, selecting Excel Documents within the Document category to organize all Excel files in the Grailer Image, and then sorting those files by last accessed date. A portion of those results are shown in **Exhibit D-17**, attached hereto, which is a series of screenshots from Axiom.

---

[25] OneDrive "SyncEngine" log files are encrypted and stored in the user's AppData folder: Users\JLGRAILER\AppData\Local\Microsoft\OneDrive\logs\Business1.

[26] Located in the Users\JLGRAILER\AppData\Local\Microsoft\OneDrive\logs\Business1 folder.

153. On page 1 of Exhibit D-17, I can see that 13 Excel files have a last accessed date within 3 seconds of each other, between 1/6/2023 at 9:03:58 AM and 9:04:00 AM (CST). I've outlined those 13 files in red in Exhibit D-17. Immediately following those 13 files, I can also see 16 Excel files that have the same last accessed date of 1/7/2023 at 12:39:26 PM (CST). I've outlined those 16 files in green in Exhibit D-17.

154. Mr. Lieb did not opine that Ms. Grailer "exfiltrated" these 29 Excel files on January 6 and 7, 2023, and he was right not to. An experienced and objective examiner would not assume, based the rapid succession of "last accessed" time stamps shown on page 1 of Exhibit D-17, that the files must have been copied to an external storage device. In fact, that hypothesis is ruled out because, just like on January 8, 2023, Digital Guardian reflected no copying to any external storage device on January 6 or 7, and further because the evidence reviewed above demonstrated that Ms. Grailer's USB thumb drive was not connected to the laptop on those days. The pattern of rapid "last accessed" time stamps shown on page 1 of Exhibit D-17 does not support an assumption that files were copied to an external storage device. Instead, it illustrates that "last accessed" time stamps are not reliable as proof of file copying.

155. On pages 2–4 of Exhibit D-17, we see Excel files that have "last accessed" time stamps between 1/8/2023 7:33:24 PM and 1/8/2023 8:50:38 PM (CST). All these files have yellow rectangles and blue rectangles next to them. The blue rectangles reflect that Mr. Lieb tagged the files as "EXFILTRATED 1/8/2023" in his Axiom Case. They are among the files listed in Mr. Lieb's Exhibit E.

156. The files on pages 2–4 of Exhibit D-17 show the same pattern of rapid "last accessed" time stamps that we saw on page 1 for January 6 and 7. This is especially true for the 55 files, listed from near the bottom of page 2 through part of page 4, that all have identical "last accessed" time stamps of 1/8/2023 8:16:17 PM (CST).

157. As with the activity on January 6 and 7, an experienced and objective forensic examiner would not conclude that this mass activity reflects copying to an external storage device. For multiple reasons, the opposite conclusion must be reached. As demonstrated above, a copying hypothesis is invalidated by the Digital Guardian report as well as the evidence showing

that Grailer's USB thumb drive was last connected on December 20, 2022. (Further, since Mr. Lieb does not claim that Ms. Grailer connected her thumb drive until 9:39:51 PM on January 8, 2023, even his account is not consistent with the hypothesis that the 1/8/2023 8:16:17 PM (CST) time stamps in Exhibit D-17 reflect files being copied to the thumb drive.)

158. In addition, even without looking at that other evidence, it is not plausible that the mass activity shown on pages 2–4 of Exhibit D-17 could reflect a user's copying activity. Pages 5 and 6 of Exhibit D-17 show the "Source" column for the 55 files with identical 1/8/2023 8:16:17 PM (CST) time stamps. That "Source" column shows the folder path for each of the 55 files.[27] As depicted on pages 5–6 of Exhibit D-17, the 55 files sharing identical 1/8/2023 8:16:17 PM (CST) time stamps are located across 33 different folders. A user could not select 55 Excel files stored in 33 different folders and copy those files to an external storage device. Further, when you look at the totality of the 33 folders, you find that (i) some of the folders contain other files not appearing in Exhibit D-17; (ii) the 33 folders are nested within approximately 4,000 OneDrive folders; and (iii) all those OneDrive folders contain over 35,000 files, consisting of over 3,200 Excel files and other various file types. It is not plausible that, within this folder structure, a user could have targeted for copying the 55 specific Excel files that share an identical 1/8/2023 8:16:17 PM (CST) "last accessed" time stamp. The time stamps clearly reflect program or service level access. As such, they are further evidence that the files were *not* copied.

159. Mass changes to "last accessed" dates result in USN change journal entries, but the analysis above illustrates why such activity cannot be relied upon as an accurate way to determine whether files were copied by a user to an external storage device. While a layperson might think that a "last accessed" time stamp would mean the last time a person accessed a file, such as copying or opening it, that is not a correct interpretation from a computer forensics perspective. Programs and services may access a file and trigger an update to a last accessed time stamp as

---

[27] Each field in the Source column starts with the forensic image and partition information as a path prefix. After "OSDisk," the field contains the folder path and file name that the user would see on the Grailer Laptop. ("OSDisk" is the volume name. The end-user would see this as drive letter C:)

well as a related entry in the USN change journal. Even at the user-level, a user previewing folders of digital photographs that are being displayed in thumbnail view can trigger an update to a last accessed time stamp, even when none of the photographs are opened by the user. Again, this is why the use of a third-party endpoint program like Digital Guardian is important—it provides a detailed event log pertaining to events where a user actually copies files to external storage media. That kind of event log cannot be reconstructed simply by assumptions based on mass file activity such as reviewed above.

The Last 23 Files in Mr. Lieb's Exhibit E

160. I also determined that the last 23 files listed in Mr. Lieb's Exhibit E were related to Ms. Grailer's receiving and sending work-related email messages on January 8, 2023. These email messages are listed in **Exhibit D-18**. File activity relating to the emails Ms. Grailer sent from her laptop's Outlook application is also referenced in the Digital Guardian report, and in my analysis of the Digital Guardian report above. As the Digital Guardian report showed, none of these files related to Ms. Grailer's emails were copied to a USB thumb drive or otherwise "exfiltrated." At the end of his Exhibit E, Mr. Lieb lists files that we can easily see were attached to emails that Ms. Grailer either received or sent on January 8, 2023. None of that email activity suggests exfiltration, let alone exfiltration to a USB thumb drive.

161. During Mr. Lieb's deposition, he was asked the following question and provided the following answer:

> *"Q. But you didn't check to see whether in your Exhibit E you might be accusing her [Ms. Grailer] of exfiltrating files that she just sent or received in her work e-mail?*
>
> *...*
>
> *A. I found no evidence of Grailer e-mailing the files that I identified in Exhibit E, your Exhibit 35, as result – a direct result of her sending an e-mail to another Ecolab employee or herself via an e-mail attachment. Because if I had, I would not have identified that file as a file I believe she exfiltrated."*

(Lieb Dep. at p. 303.)

162. Mr. Lieb's answer to that question contradicted his original declaration and expert report. In Mr. Lieb's original declaration (Lieb Decl. ¶ 39, February 21, 2023), he specifically cited email attachments as being exfiltrated, writing: "Forensic analysis of the Laptop revealed Jessica Grailer downloaded 66 email attachments from her Outlook Email account jlgrailer@ecolab.com on 1/8/2023 from 3:46:10AM to 8:50:47PM. A spreadsheet of the ***exfiltrated Email Attachments*** (emphasis added) is attached as Exhibit K and are incorporated herein by reference" (footnote omitted). Exhibit K to Mr. Lieb's declaration (Dkt. 13-14) included columns such as Timeline Category (File Download); Type (Email Attachment); and Key Detail (file names). I recognized this type of information output as an export from Axiom's Timeline View. When I checked Mr. Lieb's Axiom Case, I found that he had tagged these email attachments as "Evidence" (red icon) and "Of interest" (yellow icon).

163. The first entry in Exhibit K to Mr. Lieb's declaration was an email attachment called "3571-ILLINOIS RIVER ENERGY LLC-ROCHELLE, IL-RO2-Train A-Ecolab Global Intelligence Center Weekly Normalized Report-08-January-2023.pdf." A screenshot from Axiom Timeline is depicted in **Exhibit G-1, Figure G-1**. Mr. Lieb's tags appear to the left as red and yellow rectangles.

164. When you look at the right pane of Figure G-1, you see that this is an email attachment to an email sent by Chandrakant Bhalekar on 1/8/2023 3:49:49 AM (Email Timestamp Date/Time) and it is addressed to Jessica Grailer (jlgrailer@ecolab.com) and Brandon Schowalter (Brandon.Schowalter@ecolab.com) with a CC to System Assurance Center (SystemAssuranceCenter@nalco.com). The pane also lists a Created Date and a Modified Date, which are associated to this PDF email attachment.

165. **Figure G-2** shows basic email information about the email sent by Chandrakant Bhalekar on 1/8/2023 3:49:49 AM (CST). The attachments line shows the file names of 10 attachments. As demonstrated with the PDF attachment, each of these 10 attachments has two time stamps (Created and Modified). Since Mr. Lieb was displaying the Axiom Timeline View in Exhibit K, the first 20 entries of Exhibit K to his declaration were for these 10 email attachments (one for Created and one for Modified).

166. These 10 email attachments were not exfiltrated as Mr. Lieb claimed. Axiom categorized the email attachment event as "File Download," which Axiom defines in their User Guide as "Indicates that a file was ***downloaded from*** (emphasis added) an external source." Technically Ms. Grailer's Outlook program "downloaded" the email with the attachments when the email was synchronized to her Outlook OST File. Ms. Grailer did not exfiltrate these 10 attachments.

167. **Figure G-3** is an Axiom Timeline View that depicts an email attachment, Marquis Boiler Report_20230108.pdf, that is attached to a daily email. This is an internal email message dated 1/8/2023 5:01:53 AM (CST), addressed to Jessica Grailer, with a subject line of "enVision Report Delivery: Marquis Boiler Report." This appears to be a daily email report that is addressed to her mailbox. I searched her "Outlook OST File[28]" and found 360 emails with this same subject line. This email attachment has two time stamps, Created and Modified, and the double entry was reflected in Exhibit K to Mr. Lieb's declaration. **Figure G-4** shows basic email information about the email. Ms. Grailer did not exfiltrate this file.

168. **Figure G-5** is an Axiom Timeline View that depicts an email attachment, CHS DAILY REPORT_20230108.pdf, that was attached to a daily email. This is an internal email message dated 1/8/2023 5:03:30 AM (CST), addressed to Jessica Grailer, with a subject line of "CHS DAILY REPORT." This appears to be a daily email report addressed to her mailbox. I searched her Outlook OST File and found 359 emails with this same subject line. This email attachment has two time stamps, Created and Modified, and the double entry was reflected in Exhibit K to Mr. Lieb's declaration. **Figure G-6** shows basic email information about the email. Ms. Grailer did not exfiltrate this file.

169. **Figure G-7** is an Axiom Timeline View that depicts an email attachment, ATT00001.jpg, that is attached to an email. This is an email message dated 1/8/2023 5:31:31 AM (CST), addressed to Jessica Grailer, with a subject line of "NGG-22310 – Safety Alert -

[28] Ms. Grailer's Outlook mailbox file "jlgrailer@ecolab.com.ost" was stored in the Grailer Image.

MARQUIS ENERGY WISCONSIN LLC – NECEDAH, Wisconsin – 22310." This appears to be an email alert that was addressed to her mailbox. I searched her Outlook OST File and found 38 emails with this same subject line. This email attachment has two time stamps, Created and Modified, and the double entry was reflected in Exhibit K to Mr. Lieb's declaration. **Figure G-8** shows basic email information about the email. Ms. Grailer did not exfiltrate this file.

170. **Figure G-9** is an Axiom Timeline View that depicts an email attachment, Marquis Energy Daily MDE Report_20230108.pdf, that was attached to a daily email. This is an internal email message dated 1/8/2023 6:06:18 AM (CST), addressed to Jessica Grailer and 6 other recipients, with a subject line of "Marquis Energy Daily MDE Report." This appears to be a daily email report as I searched her Outlook OST File and found 390 emails with this same subject line. This email attachment has two time stamps, Created and Modified, and the double entry is reflected in Exhibit K to Mr. Lieb's declaration. **Figure G-10** shows basic email information about the email. Ms. Grailer did not exfiltrate this file.

171. **Figure G-11** is an Axiom Timeline View that depicts an email attachment, ATT00001.jpg, that was attached to an email. This is an email message dated 1/8/2023 10:02:50 AM (CST), addressed to Jessica Grailer, with a subject line of "NGG-8735 – Re-order Alert - MARQUIS ENERGY WISCONSIN LLC – NECEDAH, Wisconsin – 8735." This appears to be an email alert that was addressed to her mailbox. I searched her Outlook OST File and found 26 emails with this same subject line. This email attachment has two time stamps, Created and Modified, and the double entry is reflected in Exhibit K to Mr. Lieb's declaration. **Figure G-12** shows basic email information about the email. Ms. Grailer did not exfiltrate this file.

172. **Figure G-13** is an Axiom Timeline View that depicts an email attachment, ADM Clinton Cogen PSR_20230106.pdf, that was attached to an email report. This is an internal email message dated 1/8/2023 1:16:36 PM (CST), addressed to Jessica Grailer and 20 other recipients, with a subject line of "enVision Report Delivery: Nalco Water - ADM Clinton Cogen PSR." This appears to be an email report as I searched her Outlook OST File and found 108 emails with this same subject line. I found 3 copies of this email message in different folders in Ms. Grailer's Outlook OST File (Inbox\ADM Clinton\Cogen, Deleted Item, and Sync Issues). This email

attachment has two time stamps, Created and Modified, and is attached to all 3 copies; therefore, it appears as six entries in Exhibit K to Mr. Lieb's declaration. **Figure G-14** shows basic email information about the email. Ms. Grailer did not exfiltrate this file.

173. **Figure G-15** is an Axiom Timeline View that depicts one email attachment, WW trial calcs.xlsx, that was attached to an internal email sent by Ms. Grailer to Joshua Galliart. This email was sent on 1/8/2023 8:50:47 PM PM (CST), contains a total of 12 attachments (4 email messages, 5 documents, and 3 graphic files), with a subject line of "Follow Ups." What is not readily apparent in this email is that Ms. Grailer originally started this as a draft message at 5:22:01 PM (CST), which is based on the MAPI metadata field (PR_CONVERSATION_INDEX). Over the next 3 hours and 28 minutes, the attachments were added as Ms. Grailer continued to prepare this email message. The Timeline View reflected a total of 21 entries in Exhibit K to Mr. Lieb's declaration. **Figure G-16** shows basic email information about the email. Ms. Grailer did not exfiltrate these files. They were attachments to an internal email she sent to Joshua Grailer.

174. **Figure G-17** is an Axiom Timeline View that depicts one email attachment, image001.png, that was attached to an email sent by Joshua Galliart to Ms. Grailer and 9 other Ecolab recipients. This email was sent on 1/8/2023 6:04:14 PM (CST), contains one attachment, and a subject line of "FW: Sodium Nitrate shortage effecting several of our closed loop products-Place orders with additional lead time." This email attachment has two time stamps, Created and Modified, and the double entry is reflected in Exhibit K to Mr. Lieb's declaration. **Figure G-18** shows basic email information about the email. Ms. Grailer did not exfiltrate this file as it was an attachment to an internal email sent to her by Joshua Galliart.

175. **Figure G-19** is an Axiom Timeline View that depicts an email attachment, 7 DAYS REPORT-RENEWABLE ENERGY GROUP-DE FOREST Wisconsin-REG Deforest Tower-3DT007603_20230108.pdf, that was attached to a weekly email. This is an internal email message dated 1/8/2023 7:34:43 PM (CST), addressed to Jessica Grailer and 4 other recipients, with a subject line of "enVision 7 Day Report Delivery: REG - Tower." This appears to be a weekly email report that is addressed to her mailbox. I searched her Outlook OST File and found

53 emails with this same subject line. This email attachment has two time stamps, Created and Modified, and the double entry is reflected in Exhibit K to Mr. Lieb's declaration. **Figure G-20** shows basic email information about the email. Ms. Grailer did not exfiltrate this file.

176. **Figure G-21** is an Axiom Timeline View that depicts one email attachment, Chlorine Dioxide Advantages ADV-1804.pdf, that was attached to an internal email sent by Ms. Grailer to David Lucas with a CC to Joshua Galliart. This email was sent on 1/8/2023 7:55:28 PM (CST), contains a total of 3 attachments, with a subject line of "Cargill - Puris Follow Up." Ms. Grailer originally started this as a draft message at 7:39:23 PM (CST), which is based on the MAPI metadata field (PR_CONVERSATION_INDEX). The Timeline View reflected double time entries for the 3 attachments so the attachments were listed as 6 entries in Exhibit K to Mr. Lieb's declaration. **Figure G-22** shows basic email information about the email. Ms. Grailer did not exfiltrate these files. They were attachments to an internal email she sent to David Lucas and Joshua Galliart.

177. A comparison of Mr. Lieb's Exhibit K from his original declaration to Exhibit E of his expert report is attached as **Exhibit G-2**. The exhibit demonstrates that Mr. Lieb did in fact identify Ms. Grailer's email attachments as exfiltrated files not only in Exhibit K to his declaration, but also in Exhibit E to his more recent report. In Exhibit K to his declaration, he included double entries for each file as the timeline displayed both a creation date and a modification date. In Exhibit E to his report, he removed the double entries but still identified the email attachments as exfiltrated files.

178. At the conclusion of this review of email attachments, I have concluded the following:

a. Mr. Lieb identified email attachments to Ms. Grailer's work emails as "exfiltrated" files. And must have known that he was doing so, because he tagged these files in his Axiom Case as "Evidence" and "Of interest," and because he identified the files as "exfiltrated Email Attachments" in his declaration.

b. None of the email attachments Mr. Lieb identified were "exfiltrated." Ms. Grailer spent a significant amount of time between 5:22 PM and 8:50 PM drafting email

messages to Ecolab employees. She also received email messages and attachments thereto in her Ecolab inbox on January 8, 2023. None of that activity suggests "exfiltration." Mr. Lieb incorrectly interpreted the "File Download" activity related to Ms. Grailer's email attachments as exfiltration of company data.

c. Mr. Lieb testified incorrectly in his deposition when he stated that he had found no evidence of Ms. Grailer e-mailing files identified in Exhibit E to his report to other Ecolab employees, and that he would not have identified such files as "exfiltrated." Mr. Lieb accused Ms. Grailer of "exfiltrating" such work email attachments in Exhibit K to his declaration, and then he included the same files in Exhibit E to his report.

2. MTF MODIFIED DATES

179. Exhibit F to Mr. Lieb's report contains six screenshots from OSForensics. In his report, Mr. Lieb opines that "Due to the fact that it is impossible for a human being to access and open hundreds of files within seconds of each other, it is my opinion that Jessica Grailer copied these files and folders [listed in his Exhibit F] to the Emtec Drive on January 8, 2023 in addition to the files described in Exhibit E." The six screenshots in Mr. Lieb's Exhibit F depict the MFT Modified date for each file and folder listed in the exhibit. Mr. Lieb does not provide any other information or explanation in support of his expressed opinion that Exhibit F reflects copying.

180. All the January 8, 2023 time stamps in Mr. Lieb's Exhibit F occurred before 9:39:51 PM, which is when Mr. Lieb claims that Ms. Grailer connected her thumb drive to the computer. Those time stamps again reflect either program/service activity on the computer or user activity unrelated to copying. Mr. Lieb's assumption that the time stamps can only be attributed to copying has no basis and is not an assumption that an experienced and objective examiner would make. Neither I nor Mr. Lieb could determine the specific explanation for every single time stamp shown in Exhibit F without restoring the original Grailer Image to a working computer and running tests to determine the file activity of all services and programs running in the background. The copy of the Grailer Image we received from Ecolab does not permit me to do that, and it is not necessary anyway. The information provided in the copy of the Grailer Image

explains most of the time stamps that Mr. Lieb incorrectly assumes must have been copying, illustrating the unsoundness of that assumption.

181. Most of the time stamps in Mr. Lieb's Exhibit F actually demonstrate the OneDrive program in use, in this instance synchronizing folders. I will explain this in the following paragraphs.

182. Each folder synchronized with OneDrive may have multiple user files and subfolders that are synchronized with the cloud service. The synchronized folder may also be empty.

183. When a folder is selected to be synchronized with the OneDrive cloud service, a unique file named ".849C9593-D756-4E56-8D6E-42412F2A707B," which OneDrive refers to as a "Lock File",[29] is stored in the folder. Each Lock File contains a unique ID (GUID) for the synchronized folder, such as "2b0e649f-1ad4-45a1-a8bd-b4cd64570bc6" and the contents of this file matches the SyncEngine log record.

184. When the synchronized folder is updated by the OneDrive service, the service will update the MFT modified date[30] and last accessed date of the Lock File.

185. Page 1 of Mr. Lieb's Exhibit F displays a screenshot depicting the MFT Modified time stamps for a number of folders. Then, pages 2–6 of Exhibit F depict detail from five of the folders shown on the exhibit's page 1.

186. The majority of the MFT Modify Date entries on pages 1, 4, and 6 of Mr. Lieb's Exhibit F display as 1/8/2023 at approximately "12:41 PM." Those times, however, are off by one hour, because Mr. Lieb set the time zone offset incorrectly when he prepared the OSForensics screenshots. Mr. Lieb had the offset at UTC-5, which is appropriate for Central *Daylight* Time.

---

[29] OneDrive records activity in the SyncEngine logs. An example of the Lock File is the log file containing a function called "LockFileManager::ReadLockFile," and the Params_Decoded field will reference the contents of a Lock File, such as "{"guid" : "2b0e649f-1ad4-45a1-a8bd-b4cd64570bc6","version" : 1}"

[30] The NTFS file system has four different time stamps for each file listed in the Master File Table (MFT): File Created, Last Modified, Last Accessed, and MFT Modified. There is record for each file and folder in the MFT. The MFT Modified time stamp is updated when a change has occurred to an attribute in the MFT record.

But in January, the correct offset is UTC-6 (Central Standard Time). Thus, the "12:41 PM" times in Mr. Lieb's exhibit should instead read 11:41 AM (CST, UTC-6). The remaining dates in the exhibit must be similarly adjusted. I confirmed this by checking the Grailer Image with OSForensics version 10.0.1016, with the time zone set to CST. It displayed the correct time of 11:41 AM. To depict the correct time stamps, I then replicated Mr. Lieb's screenshots using OSForensics and attached them hereto as **Exhibit D-19**. Exhibit D-19 also includes additional information ("date modified" and "date accessed" time stamps) that was not included in Mr. Lieb's Exhibit F. I will continue to use Exhibit D-19 below, not Mr. Lieb's Exhibit F, so we can consider the accurate time stamps.

187. Looking at Exhibit D-19, the folders with 11:41 PM time stamps all have something in common: each folder is synchronized and contains a OneDrive Lock File. **Exhibit D-20** contains a listing of the OneDrive Lock Files (each of which has the same file name) along with the Last Accessed and MFT Modified time stamps, and the synchronized folder where each Lock File is stored. I also note that:

a. Exhibit D-20 displays three folders at the bottom that do not have a last accessed or MFT modified date of 1/8/2023. Those three folders are empty.

b. Pages 2, 3, 4, and 6 of Exhibit D-19 depict the ".849C9593-D756-4E56-8D6E-42412F2A707B" OneDrive Lock File. The same is true of pages 2, 3, and 4 of Mr. Lieb's Exhibit F. (The last page of Mr. Lieb's Exhibit F is truncated, so the file does not show on that page.) Page 5 of Exhibit D-19 and Mr. Lieb's Exhibit F do not show the OneDrive Lock File because on that page, Mr. Lieb took a screenshot of a subfolder of the parent folder that contains the OneDrive Lock File.

c. Page 1 of Exhibit D-19 and Mr. Lieb's Exhibit F depict four other folders that do not have a MFT Modified date of 1/8/2023. The "Guy, Valleri - WL143" and "Pollitz, Eric - NA Light Pricer Tool" folders are both empty, and the MFT Modified time stamp matches the last time those folders were synchronized. The "PRO" and "CWO" folders are not synchronized.

188. What we see, on pages 1, 4, and 6 of Exhibit D-19 and Mr. Lieb's Exhibit F is the MFT Modify Date for folders being changed due to OneDrive's folder synchronization activity. It should also be noted that this OneDrive information was not missing from Mr. Lieb's Axiom Case. Axiom parsed out this information into a category called "Cloud Storage, One Drive." **Exhibit C, Figure 25** depicts a portion of the information displayed in the Axiom Case, including the Lock Files, the last modified dates, the "owner" of the OneDrive folder, and the full path of the Lock Files.

189. Another (but different) example of background services/programs touching files in the OneDrive folder can be seen in file activity from February 8, 2023, when the computer was in Mr. Lieb's custody, before it was imaged. As depicted in **Exhibit D-21**, from 3:49:58 PM to 4:01:56 PM, 320 subfolders within the OneDrive folders were accessed.

190. As demonstrated above, program and system activity can play a role in file system date and time stamps. For this reason, grouping files and folders by time stamps is not indicative of user-related file copying activity. The operating system, installed software, and services play a role in altering time stamps of files. The folders cited in Mr. Lieb's Exhibit F illustrate that point.

191. A user's work-related file activity can also play a role. An example of specific user activity related to time stamps depicted in Exhibit D-19 would be found on page 5 of the exhibit, which shows the names of files in the following folder: \Users\JLGRAILER\Ecolab\Taverna, Andrew - ADM 500072855\Waste Water. That folder shows "MFT Modified Dates" for multiple files on January 8, 2023 at 5:27:18 PM (CST) and an MFT Modified Date for the "April 2022" subfolder on January 8, 2023 at 5:27:53 PM (CST).

192. An examiner can find examples of a user's recent file activity by looking at file activity captured by the Windows browser (Edge/Internet Explorer), Windows-created LNK files, and Windows-created "Jumplists." This type of activity is organized by Axiom. The Digital Guardian report can also be used to view a user's file activity. Here, we can see file activity by Ms. Grailer showing that she was working in the Users\JLGRAILER\Ecolab\Taverna, Andrew - ADM 500072855\Waste Water folder and its "April 2022" subfolder around 5:27 PM (CST) on January 8.

193. For example, the Windows browser history, which includes Windows Explorer file activity, shows that Ms. Grailer opened an Excel file called "oin.xlsx," on 1/8/23 at 5:27:33 PM (see **Exhibit E, Figure E-1**). This file was located in the following folder: \Users\JLGRAILER\Ecolab\Taverna, Andrew - ADM 500072855\Waste Water\April 2022. In Exhibit E, Figure E-1, you can see a yellow tag ("Of Interest") that Mr. Lieb created. This entry was stored in a Windows file called V01.log. A second entry is listed in Figure E-1 for the same file, date, and time, which was stored in a separate Windows file called WebCacheV01.dat.

194. A Windows LNK file was also created by Windows that shows that Ms. Grailer opened the same Excel file (oin.xlsx), located in the same folder listed above, on 1/8/23 at 5:27:33 PM (see **Exhibit E, Figure E-2**). A Windows LNK file is a Windows-created shortcut that the user can access to re-open a recently accessed file. The creation date of this file is the time when the user opened the file. The "Target File" references in Figure E -2 refer to the Excel file itself, such as when the Excel file was created, modified, last accessed, and the size of the file (in this case 14,906 bytes).

195. A Windows Jumplist file entry also was created by Windows that shows that Ms. Grailer was accessing the "April 2022" folder (\Users\JLGRAILER\Ecolab\Taverna, Andrew - ADM 500072855\Waste Water\April 2022) on 1/8/23 at 5:27:33 PM (see **Exhibit E, Figure E-3**). Windows Jumplist files store a user's recent file and folder activity.

196. A Windows Jumplist file entry was further created by Windows that shows the Ms. Grailer was accessing an Excel file (WW trial calcs.xlsx), located in the "April 2022" folder on 1/8/23 at 5:27:33 PM (see **Exhibit E, Figure E-4**). A closer look at the Windows LNK file entry and this Jumplist file entry, you can see that what appears to be two different files based on file name are actually the same file (see **Exhibit E, Figure E-5**). The "Target File" creation date, last modified date, and file size are the same. However, the last accessed times are different (5:27:33 PM and 5:27:53 PM). The difference in the time stamps is because the file was renamed from "oin.xlsx" to "WW trial calcs.xlsx." This information is contained in a OneDrive SyncEngine log file (SyncEngine-2023-01-08.2248.10312.30.odlsent), which contains a record dated 2023-01-08 23:27:53.680000 (UTC), which is 1/8/23 at 5:27:53 PM (CST), and the

Params_Decoded field displays "['FILE_ACTION_RENAMED_NEW_NAME', '%MountPoint%[7c16262bf3574f3c8e28f0d98c1cab5c]\\Waste Water\\April 2022\\WW trial calcs.xlsx']." Furthermore, this renaming activity can be corroborated by reviewing the Digital Guardian Report for the event occurring on 1/8/2023 at 5:27:53 PM.

197. **Exhibit E, Figure E-6** shows the files contained in the "April 2022" folder, which includes the Excel file, WW trial calcs.xlsx.

198. The USN change journal shows activity with the "WW trial calcs.xlsx" file in the user's temporary folder associated with Microsoft Outlook (\Users\JLGRAILER\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\2EEDJ9XY), "INetCache Folder," between 1/8/2023 7:58:01 PM and 1/8/2023 8:50:39 PM. The INetCache Folder is depicted in **Exhibit E, Figure E-7**.

199. The "WW trial calcs.xlsx" file was one of multiple email attachments that Ms. Grailer sent in an email with a subject line of "Follow Ups" to Joshua Galliart on 1/8/23 at 8:50:47 PM, which is reflected in Exhibit D-18. This activity is also reflected in the Digital Guardian report.

200. This timeline demonstrates what started with Ms. Grailer working with one Excel file, "oin.xlsx," renaming it to "WW trial calcs.xlsx," and eventually attaching it to an email to Joshua Galliart. The "WW trial calcs.xlsx" file is one of the files that Mr. Lieb claims Ms. Grailer exfiltrated to a USB thumb drive on January 8, 2023 (even though not even Mr. Lieb claims that that thumb drive was connected during the activity reviewed above), but digging into the available data allows an examiner to see that Ms. Grailer was using the file and sending it to an Ecolab recipient, not "exfiltrating" it.

201. As demonstrated above, tracing date and time stamp activity can be exhausting when looking at the active roles played by program activity, system activity, and a user's activity. But the action of "exfiltrating" files to a USB thumb drive can be ruled out in this instance since an external storage device was not connected to the computer after December 20, 2022 and the Digital Guardian report showed no indication of files being copied to any external storage device.

II. LIEB'S INTERPRETATION OF THE MICROSOFT OFFICE 365 AUDIT LOG

202. In his report, Mr. Lieb opines that "Ecolab preserved an Office365 User Activity Log ('Log') capturing the fact that a person (whom [Mr. Lieb] assume[d] to be Jessica Grailer) accessed her former Ecolab OneDrive account on January 11, 2023, January 12, 2023, January 13, 2023, January 14, 2023, January 15, 2023, January 16, 2023, January 17, 2023 and January 18, 2023 using an undisclosed computer ('Undisclosed Computer')." (Lieb Report ¶ 22.)

203. Mr. Lieb further opines that "as seen in" the log, "Jessica Grailer accessed [20 specific] files stored in her Ecolab OneDrive account on January 15, 2023 using the Undisclosed Computer." (Lieb Report ¶ 23.) Mr. Lieb lists those 20 files in Table 1 in his report. (Lieb Report ¶ 23, Table 1.) He opines that Ms. Grailer was "in possession of" the files on January 15, 2023. (Lieb Report ¶ 27.)

204. Additionally, Mr. Lieb opines that the log "also contains evidence that Jessica Grailer attempted to access her former Ecolab OneDrive account on January 11, 2023, January 14, 2023, and January 16, 2023, using a personally owned Apple iPhone 12 Mini, but was unable to login to the account using her Apple iPhone 12 Mini." (Lieb Report ¶ 24.)

205. Finally, Mr. Lieb opines that "the Ecolab OneDrive Log shows that Jessica Grailer successfully logged in and opened and deleted files on multiple dates after her resignation on January 8, 2023, and through the use of an Undisclosed Computer." (Lieb Report ¶ 30.) Mr. Lieb offers no specifics about when he claims that Ms. Grailer "logged in and opened and deleted" such files, or which specific files he claims she opened and deleted.

206. None of these expressed opinions have any basis in the O365 Audit Log. I will explain this below. In Section A, I begin by addressing significant problems with Mr. Lieb's failure even to correctly identify the O365 Audit Log, or to rely upon the correct log when forming his opinions. Then in Section B, I address what the O365 Audit Log actually shows.

A. IDENTIFYING THE CORRECT MICROSOFT OFFICE 365 AUDIT LOG

207. I must begin by addressing which file contains the Microsoft Office 365 audit log that Mr. Lieb should have been reviewing. The answer is the "O365 Logs for Grailer.xlsx" file

(the "O365 Audit Log") that Ecolab's counsel provided by email on August 16, 2023. Mr. Lieb, however, acknowledged in his deposition that he (incorrectly) relied on a different file instead.

208. In May 2023, Ecolab's counsel provided a heavily filtered version of the data that is contained in the O365 Audit Log. Ecolab's counsel provided that filtered version on May 3, 2023, in a file called "JGrailer.xlsx" (the "Filtered Log"). Screenshots showing all the data available in the "Filtered Log" are shown in Exhibit 9 to Mr. Lieb's deposition, which I have attached hereto as **Exhibit D-22**. As shown there, the Filtered Log contained only 6 of the O365 Audit Log's many columns of data. The Filtered Log's rows also covered only the period from January 11 through the morning of January 18, 2023. The O365 Audit Log begins on January 8, 2023 and also includes entries from later in the day on January 18, 2023 that were not included in the Filtered Log.

209. An experienced and objective examiner would consider the O365 Audit Log (although as I discuss below even the O365 Audit Log appears on detailed review to have gaps) and would not consider relying upon the Filtered Log. An experienced and objective examiner would have easily recognized the Filtered Log as an incomplete extraction of the available log data. Provided with the Filtered Log, an experienced and objective examiner would ask for the data that was clearly missing.

210. Mr. Lieb, however, testified in his deposition that he relied on the Filtered Log both in his February 2023 declaration and in his report. (Lieb Dep. at pp. 89–90, 108–112.) He also testified that he did not receive the O365 Audit Log until sometime in the fall of 2023 and that, during the months when he had the Filtered Log but not the O365 Audit Log, he did not feel he was missing relevant information. (Lieb Dep. at pp. 105, 114.) Further, as noted in my section above about Digital Guardian, Mr. Lieb testified that when preparing his February 2023 declaration, he "assumed" that the Filtered Log had come "from Digital Guardian," even though it clearly had not. (Lieb Dep. at pp. 88–91, 103.)

211. These errors by Mr. Lieb are very problematic. An experienced and objective examiner would have understood from the beginning that Plaintiffs had failed to provide available audit log data, and would have obtained that data before forming opinions. An experienced and

objective examiner also would never have mistaken the Filtered Log for a Digital Guardian report. And an experienced and objective examiner of course would not rely on data such as that shown in Exhibit D-22 when the examiner did not know the data's origin. But Mr. Lieb made all these mistakes. And, as we will see below, his failure to obtain the log data available to him before forming his opinions contributed to the many substantive mistakes that Mr. Lieb made in interpreting the obviously incomplete data that he relied upon.

212. Two of those substantive mistakes are acknowledged even by Mr. Lieb. First, in his February declaration, Mr. Lieb relied on the Filtered Log (which he then assumed had come from Digital Guardian) to support his testimony that Ms. Grailer "access[ed] her Ecolab OneDrive account using a heretofore undisclosed iPhone 12 Mini on Jan 14, 2023 @ 00:52:28.000." (Lieb Decl. ¶ 16, February 21, 2023.) That testimony had no basis in the Filtered Log—which depicted a "UserLogin*Failed*" event on Jan 14, 2023 @ 00:52:28.000, not account *access*—and Mr. Lieb backed away from it in his report. In his report, he opined that Ms. Grailer did *not* (and *could not*) access her Ecolab OneDrive account using her iPhone 12 Mini on January 11, 14, or 16, 2023. (Lieb Report ¶¶ 24–25, 30.)

213. Second, as noted above, Mr. Lieb opined in his report that the Filtered Log showed that Ms. Grailer "deleted files on multiple dates after . . . January 8, 2023." (Lieb Report ¶ 30.) When confronted with the larger O365 Audit Log during his deposition, Mr. Lieb agreed that this opinion was wrong in at least one respect: the deletions he'd referred to regarded *Outlook calendar events*, not "files." As Mr. Lieb explained in his deposition, the Filtered Log referenced a series of "HardDelete" events, but it omitted the columns showing that the "HardDeleted" items were Outlook calendar events. (Lieb Dep. at pp. 126–127.) Lacking that information, Mr. Lieb apparently jumped to the incorrect conclusion that the "HardDeleted" items must have been files. In reality, the log entries were about Outlook calendar events. I will discuss the O365 Audit Log's "HardDelete" entries in more detail below.

B. WHAT THE O365 AUDIT LOG SHOWS

214. I reviewed the O365 Audit Log. Below, I separately address Mr. Lieb's allegations that (i) "a person (whom [Mr. Lieb] assume[d] to be Jessica Grailer) accessed her former Ecolab

OneDrive account on January 11, 2023, January 12, 2023, January 13, 2023, January 14, 2023, January 15, 2023, January 16, 2023, January 17, 2023 and January 18, 2023 using an undisclosed computer ('Undisclosed Computer')"; (ii) that "Jessica Grailer accessed [20 specific] files stored in her Ecolab OneDrive account on January 15, 2023 using the Undisclosed Computer," and was "in possession of . . . [those] Ecolab files . . on January 15, 2023"; (iii) that Jessica Grailer attempted to access her former Ecolab OneDrive account on January 11, 2023, January 14, 2023, and January 16, 2023, using a personally owned Apple iPhone 12 Mini, but was unable to login to the account using her Apple iPhone 12 Mini"; and (iv) that Jessica Grailer successfully logged in and opened and deleted files on multiple dates after her resignation on January 8, 2023, and through the use of an Undisclosed Computer." (Lieb Report ¶¶ 22–24, 27, 30 & Table 1.) I will address each of those four allegations in the four subsections below.

1. ACCOUNT ACCESS DURING JANUARY 11–18, 2023

215. The O365 Audit Log is clear that the last time anyone logged into Ms. Grailer's Ecolab Microsoft account was January 8, 2023. The O365 Audit Log directly refutes Mr. Lieb's claim that a person accessed the account between January 11 and 18, 2023.

216. The successful and unsuccessful login events shown in the O365 Audit Log are depicted in **Exhibit D-23**. This exhibit, which is an excerpt from the O365 Audit Log, contains the date and time; the IP address of the device; the event action and corresponding outcome; the user ID (jlgrailer@ecolab.com); and, the user agent information, which describes the device used in the login event.

217. As shown in Exhibit D-23, throughout January 8, 2023, Ms. Grailer logged into her Ecolab Microsoft account with her user ID as "jlgrailer@ecolab.com." After that date, the log shows that her mobile device (Apple iPhone) was attempting to login; however, as Mr. Lieb agrees, those logins were unsuccessful. The O365 Audit Log shows no successful logins after January 8, 2023.

218. In his report, Mr. Lieb did not mention the obviously relevant fact that the O365 Audit Log shows successful login events throughout January 8, 2023, but no such login events

after January 8, 2023. We learned in his deposition that this is because Mr. Lieb was relying on the Filtered Log, which, unlike the O365 Audit Log, included no data from January 8.

219. During his deposition, Mr. Lieb offered two different explanations for the lack of any "UserLoggedIn" events after January 8, 2023. First, when looking only at the Filtered Log, which had data going back only to January 11, Mr. Lieb testified that it looked to him like the log may have been recording only failed login events, not successful login events. (Lieb Dep. at pp. 128–129.) That testimony was incorrect because, as discussed above and depicted in Exhibit D-23, the O365 Audit Log recorded numerous "UserLoggedIn" events on January 8, 2023.

220. Second, when confronted with the fact that the O365 Audit Log recorded "UserLoggedIn" events on January 8, 2023, but no such events after that day, Mr. Lieb claimed that the O365 Audit Log did not record the *device* Ms. Grailer used for each successful "UserLoggedIn" events, and testified that his "best explanation" was that Ms. Grailer may have used an unidentified device (not her work computer) to generate one of those "UserLoggedIn" events. (Lieb Dep. at pp. 133–142.) Again, all the "UserLoggedIn" events shown in the O365 Audit Log occurred on January 8, 2023. Mr. Lieb testified that one of those January 8 "UserLoggedIn" events could have originated from an unidentified device, and that Ms. Grailer could have allowed that unidentified device to remain logged in through January 15, 2023 or perhaps later. (Lieb Dep. at pp. 133–142.)

221. Mr. Lieb identified no evidence to support his last claim (or evidence that it even would have been possible for Ms. Grailer to log in to her account from a device Plaintiffs cannot identify and to sustain a single login session for one week or more), and the O365 Audit Log shows that he was wrong. The O365 Audit Log did in fact record the device used for each of Ms. Grailer's "UserLoggedIn" events. This is shown in **Exhibit D-24**, attached hereto, which depicts the same successful and unsuccessful login events shown in Exhibit D-23, except with the O365 Audit Log's "DeviceProperties.Value" column shown. The Grailer Laptop was assigned a Windows computer name of "USNB190410TOH6X." The O365 Audit Log recorded that computer name in the "DeviceProperties.Value" column for all of Ms. Grailer's "UserLoggedIn" events, as shown in Exhibit D-24. The O365 Audit Log would have made a record if Ms. Grailer

had logged in from a different device. The fact that it did not make a record of any such other device disproves Mr. Lieb's speculation. Mr. Lieb's conjecture about an "undisclosed" computer is contradicted by all the available evidence.

2. FILE ACCESS ON JANUARY 15, 2023

222. The O365 Audit Log is also clear that no one used Ms. Grailer's Ecolab Microsoft account to access files on January 15, 2023. The O365 Audit Log records a total of 37 similar Sharepoint events (all of them "FilePreviewed" events) on January 9, 2023 and January 15, 2023. In claiming that Ms. Grailer accessed files on January 15, 2023, Mr. Lieb must be referring to the January 15, 2023 Sharepoint "FilePreviewed" events. He does not discuss the similar Sharepoint "FilePreviewed" events on January 9, 2023. I will discuss both sets of events below.

223. A "FilePreviewed" event is defined as an event where a "User previews files on a SharePoint or OneDrive for Business site."[31] As Microsoft explains, "FilePreviewed" events "typically occur in high volumes based on a single activity, such as viewing an image gallery" (same citation). In other words, consistent with Microsoft's explanation and my own experience reviewing audit logs for OneDrive and Sharepoint, "FilePreviewed" events are typically related to thumbnail images of files being displayed, not to files being accessed, copied, or downloaded. Microsoft uses different event codes such as "FileAccessed," "FileCopied," "FileDownloaded" for such other events (same citation).

224. The O365 Audit Log shows that on January 9, 2023, within two seconds (15:51:56 to 15:51:57), thumbnail images for 17 files located in 5 different non-public Uniform Resource Locators (URLs) (o365.audit.SiteUrl) were displayed by a Microsoft application called "PeoplePredictions" (o365.audit.ApplicationId = 35d54a08-36c9-4847-9018-93934c62740c).[32]

225. Similarly, the O365 Audit Log shows that on January 15, 2023, within two seconds (13:01:37 to 13:01:38), thumbnail images for 20 files located in 8 different non-public URLs were displayed by the same Microsoft application called "PeoplePredictions."

---

[31] https://learn.microsoft.com/en-us/purview/audit-log-activities
[32] https://learn.microsoft.com/en-us/troubleshoot/azure/active-directory/verify-first-party-apps-sign-in

226. Since the Sharepoint sites (URLs) containing these files are non-public, a user would have to login to the site with valid user credentials to gain access. These 37 events list the user account (user.id) as jlgrailer@ecolab.com. However, as shown in Exhibits D-22 and D-23, there are no successful logins for Ms. Grailer's user ID after January 8, 2023. Further, every successful login that the log shows for Ms. Grailer's user ID were logins from Ms. Grailer's Ecolab laptop. The log does not show any logins from any other device, contrary to Mr. Lieb's non-evidence-based speculation about an "undisclosed" computer logging in. Ms. Grailer still had her Ecolab laptop on January 9, but the Grailer Image shows it was offline and not running at the time of the January 9 Sharepoint "FilePreviewed" events. And by January 15, the laptop was both offline and in Plaintiffs' custody. The Sharepoint "FilePreviewed" events on January 9 and 15, 2023 were clearly not related to user access to Ms. Grailer's account.

227. In his report, Mr. Lieb claimed that an "Undisclosed Computer" generated the "FilePreviewed" events on January 15, 2023. (Lieb Report ¶ 22.) That claim is falsified by the lack of any log record showing another computer logging in. In addition, the O365 Audit Log shows that the 37 Sharepoint "FilePreviewed" events, on both January 9 and 15, 2023, all had the same source IPv6 Internet address of 2603:1036:301:225c::5, and the same geolocation in Des Moines, IA. That IP address is registered to Microsoft Corporation.

228. Through this data, none of which Mr. Lieb addresses in his report, the O365 Audit Log demonstrates that a Microsoft system using PeoplePredictions accessed a Microsoft Sharepoint cloud service in 2-second increments on two separate days, and that Ms. Grailer was not logged in at the time of these events. Ms. Grailer is not responsible for the January 9 and January 15 events. As shown in Exhibits D-23 and D-24, there are no successful logins for Ms. Grailer's user ID after January 8, 2023.

229. Further, even if the January 9 and January 15 events were associated with user access to Ms. Grailer's account, which they are not, Mr. Lieb still would have been wrong to conclude that the events involved Ms. Grailer "accessing" or gaining "possession" of the referenced files. Again, as Microsoft explains, "FilePreviewed" events typically are related to thumbnail images of file being displayed, not to files being accessed, copied, or downloaded. The

O365 Audit Log and the Filtered Log both show that the January 15, 2023 events were "FilePreviewed" events, but Mr. Lieb does not discuss that fact or address the meaning of "FilePreviewed" in his report.

3. THE "UserLoginFailed" EVENTS FROM MS. GRAILER'S PHONE

230. As shown in Exhibits D-23 and D-24, the O365 Audit Log records "UserLoginFailed" events that were generated by Ms. Grailer's iPhone on January 10, 11, 14, and 16. Mr. Lieb mentions the January 11, 14, and 16 events in his report, but not the earlier January 10 event (which is recorded in the O365 Audit Log but was not included in the Filtered Log).

231. The O365 Audit Log is clear that Ms. Grailer's iPhone generated the "UserLoginFailed" events. According to the O365 Audit Log, the login events failed due to an "InvalidUserNameOrPassword" (o365.audit.Logon.Error = "InvalidUserNameOrPassword").

232. The O365 Audit Log, however, also tells us that Ms. Grailer's phone was specifically attempting to login to Plaintiffs' Microsoft Exchange (email) service. The login activity recorded in the O365 Audit Log was application specific—*i.e.,* each login was connected to a particular application such as Microsoft Sharepoint or Microsoft Exchange. A column in the O365 Audit Log that is not depicted in Exhibits D-23 or D-24—the column is called "o365.audit.ApplicationId"—identifies the application that Ms. Grailer's phone attempted to log into for each "UserLoginFailed" event as "00000002-0000-0ff1-ce00-000000000000." The "00000002-0000-0ff1-ce00-000000000000" ID refers to the Office 365 Exchange Online application.[33] In other words, Ms. Grailer's phone was simply attempting to login to Ms. Grailer's email and calendar.

233. The O365 Audit Log does not tell us whether or not Ms. Grailer herself tried to cause her phone to log in to her email and calendar. "UserLoginFailed" events like those shown in Exhibits D-23 and D-24 can be associated with a user entering invalid login credentials, but they can also reflect an application that is installed on the phone attempting to log in on its own.

[33] https://learn.microsoft.com/en-us/troubleshoot/azure/active-directory/verify-first-party-apps-sign-in

The O365 Audit Log does not tell us which scenario applied to the "UserLoginFailed" events that it recorded.

4. THE O365 AUDIT LOG'S "HardDelete" EVENTS

234. The O365 Audit Log shows 102 log events not discussed above that occurred between January 9, 2023 and January 18, 2023 and were also related to Ms. Grailer's user ID. Those events were associated with Plaintiffs' Microsoft Exchange (email) service. Specifically, the 102 log events recorded "HardDelete" actions of calendar events. As noted above, Mr. Lieb was referring to these events when he opined in his report that "the Ecolab OneDrive Log shows that Jessica Grailer successfully logged in and opened and deleted files on multiple dates after her resignation on January 8, 2023, and through the use of an Undisclosed Computer." (Lieb Report ¶ 30.)

235. The "HardDelete" log entries do not show Ms. Grailer logging in to her Microsoft account or opening any files. They do not even show any files being deleted. Instead, they record the deletion of calendar events within Plaintiffs' Microsoft Exchange (email) service.

236. In addition to reviewing the O365 Audit Log, I processed Ms. Grailer's Outlook mailbox file ("Outlook OST File") stored in the Grailer Image, "jlgrailer@ecolab.com.ost." I extracted the mailbox content, including metadata, from the Outlook OST File using Metaspike Forensic Email Intelligence, version 2.1.14.12.

237. During Mr. Lieb's deposition, he stated that he did not know what the term "HardDelete" meant in the O365 Audit Log. (Lieb Dep. at pp. 116, 118, 181.) Since he did not know, I will explain it below.

238. All 102 deleted ("HardDelete") calendar events are related to the shared calendars of two Ecolab employees, Patrick M Severson and Benjamin Irwin. This fact is evident in the O365 Audit Log field called "o365.audit.AffectedItems.ParentFolder.Path." This field along with 7 other relevant fields contained within the O365 Audit Log are attached hereto as **Exhibit D-25**. When another employee shares their calendar, the employee sharing the calendar has the option of setting the permissions of how the calendar events are shared with others in the organization.

239. Before explaining the details of shared calendar events in the O365 Audit Log, I need to explain the cause and effect of an employee sharing calendar events with another employee. When Employee A creates or accepts a calendar event, that event is stored in Employee A's calendar. If Employee A shares their calendar with Employee B, Employee B's mailbox account will automatically generate a new, matching calendar event and display the new, matching calendar event in Employee B's calendar. If Employee A deletes the calendar event, Employee B's mailbox account will automatically delete the matching calendar event from Employee B's calendar. In short, Employee A initiates the action of creation and deletion of a calendar event and Employee B's mailbox account automatically matches the action on the matching calendar event. This type of activity is explained in detail below:

a. The 48 deleted calendar events listed in the O365 Audit Log for Mr. Severson displayed a subject line of "Busy," "Tentative," or were blank. This is consistent with a shared calendar that only allows "people you share with can only see the times you have blocked out as busy." Whenever Mr. Severson would create or accept a calendar event in his calendar, the event entry would be marked as "Busy," "Tentative," "Free," or "Out of Office." In turn, Ms. Grailer's email account would automatically create a new, matching calendar event with limited information and display that event in the calendar in her mailbox.

b. An example of a shared calendar event for Mr. Severson's is depicted in **Exhibit F, Figure F-1**. This calendar event was stored in the Outlook OST File and was also listed as deleted in the O365 Audit Log. The event displays "Busy" as the subject line and is scheduled for January 11, 2023 4:30:00 PM (-06:00). For reference, this event was automatically generated by Ms. Grailer's email account on 1/5/23 at 2:34:00 PM (CST) with a Message ID of DM6PR06MB604253B24335EA959F33D9E8D3FA9@DM6PR06MB6042.namprd06.prod.outlook.com.[34]

[34] This calendar metadata information is referenced from the following two MAPI fields: PR_CLIENT_SUBMIT_TIME and PR_INTERNET_MESSAGE_ID_W.

c. Based on the O365 Audit Log, this calendar event with matching Message ID[35] was deleted ("HardDelete") on 1/18/2023 at 4:13:56 PM (CST). The audit log shows the deletion is associated with Ms. Grailer's account because this event was automatically created by her mailbox account on 1/5/2023 due to Mr. Severson creating the calendar event. Mr. Severson likely deleted this event from his calendar later, which, in turn, caused Ms. Grailer's account to automatically delete the event.

d. The 54 deleted calendar events listed in the O365 Audit Log for Mr. Irwin functioned the same way as the calendar events for Mr. Severson. An example of a shared calendar event for Mr. Irwin is depicted in **Exhibit F, Figure F-2**. This calendar event was stored in the Outlook OST File and was also listed as deleted in the O365 Audit Log. This event displays "Rich Foods - Brandon contacts list to Maddie and Steve" as the subject line and was scheduled for January 9, 2023 11:30:00 AM (-06:00). For reference, this event was automatically generated by Ms. Grailer's email account on 1/8/2023 at 8:03:32 PM (CST) with a Message ID of BN8PR06MB5714104D88E9540C907A118CFEF99@BN8PR06MB5714.namprd06.prod.outlook.com.[34]

e. Based on the O365 Audit Log, this calendar event with matching Message ID was deleted ("HardDelete") on 1/9/2023 at 9:30:43 AM (CST). The audit log shows the deletion is associated with Ms. Grailer's account because this event was automatically created by her mailbox account on 1/8/2023 due to Mr. Irwin creating the calendar event. Mr. Irwin likely deleted this event from his calendar later, which, in turn, caused Ms. Grailer's account to automatically delete the event.

240. I note one final issue before turning away from the O365 Audit Log. It is my understanding that the O365 Audit Log provided by Plaintiffs' counsel was supposed to contain all O365 audit log entries for Ms. Grailer's activity January 8 through January 18. However, I have already found that log entries which should be included were apparently omitted instead. For

---

[35] See O365 Audit Log field "o365.audit.AffectedItems.InternetMessageId"

example, an O365 audit log typically would include additional events for Exchange email activity such as: (i) the creation and updating of calendar events; and (ii) the creation and sending of email messages. I found evidence of Ms. Grailer creating and sending email messages to Ecolab employees as described in paragraph 36 above. These events were not included in the O365 Audit Log. Furthermore, I conducted an analysis of the O365 Audit Log and compared the MessageIDs of each deleted calendar event (48 deleted entries for Mr. Severson and 54 deleted calendar entries for Mr. Irwin) to the MessageIDs of the calendar events stored in the Outlook OST File. The Outlook OST File contained only one matching MessageID for Mr. Severson and only 33 matching MessageIDs for Mr. Irwin. This comparison implies that the "unmatched" calendar events occurred after January 8, 2023 as Ms. Grailer's mailbox could not synchronize those events to the Outlook OST File as the computer was offline. The creation of these "unmatched" calendar events do not appear in the O365 Audit Log. During the evening of January 8, 2023, there were 9 shared calendar events for Mr. Irwin and Mr. Severson. None of these events appeared in the O365 Audit Log. I understand that Plaintiff entered a stipulation regarding the O365 Audit Log as "an accurate reproduction of the data that would have been in an audit log had the Microsoft Compliance Portal been used to directly export the audit log data." Unfortunately, the evidence suggests this may not be accurate, and it is unknown what other events may be missing.

III. RECYCLE BIN ACTIVITY

241. Mr. Lieb stated in his report that "Jessica Grailer deleted hundreds of files from her Ecolab Laptop on the evening of January 8, 2023," and that the "files that were deleted on the evening of January 8, 2023" are listed in Exhibit G to Mr. Lieb's report. (Lieb Report ¶ 20 & Ex. G.) This is not a reasonable or accurate account of what the evidence in the Grailer Laptop actually shows.

242. I examined the recycle bin activity for the Grailer Laptop, which included the USN change journal and recycle bin files.

243. When a user deletes a file, the file is moved from the original folder where it was stored to the user's recycle bin folder.[36] When the file is moved, it is renamed from the original file name to a new file name that starts with a $R prefix and 6 random alpha-numeric characters. It keeps the original file extension. Windows then creates a recycle bin information file that contains the date/time of deletion, the size of the file, and the original file name and folder of where the file was stored. The recycle bin information file starts with a $I prefix and then matches the new file name that was assigned (6 random alpha-numeric characters and the original file extension).

244. For example, on 1/8/2023 at 8:55:25 PM (CST), Ms. Grailer deleted a file called "Passwords - Copy.docx," which was stored in the \Users\JLGRAILER\OneDrive - Ecolab\Desktop\desktop folder. The file was moved to her recycle bin folder and renamed to "$RCEI1XS.docx." A recycle bin information file called $ICEI1XS.docx was also created and saved in the recycle bin folder.

245. USN change journal entries show that on January 8, 2023, between 1/8/2023 8:52:25 PM and 1/8/2023 9:04:37 PM (CST), Ms. Grailer deleted 21 files. A list of those files is attached hereto as **Exhibit D-26**. They include the "Passwords – Copy.docx" file that I used as an example in the paragraph above.

246. By reviewing OneDrive SyncEngine logs, I also found that a folder called "payslips" was deleted from the \Users\JLGRAILER\OneDrive - Ecolab\Desktop folder at approximately 8:48 PM (CST). This folder contained files such as:

a. Payslip - December 2022.PNG;

b. Payslip - January 2020.html (along with web-based code files in a subfolder called "Payslip - January 2020_files);"

c. Payslip - January 2020.PNG;

d. DrugScreenRegistrationInstructions.pdf;

---

[36] Ms. Grailer's recycle bin folder was \$Recycle.Bin\S-1-5-21-3343834222-2031793820-3172701118-375185

e. 2013 W2.jpeg;

f. W2 2019.PNG; and,

g. ePassport_WD-121822-5U2YD.pdf.

247. Ms. Grailer began to delete files from the recycle bin between 8:59 PM and 9:05 PM (CST). I recovered 39 information files ($I files) from Ms. Grailer's recycle bin folder and found that her recycle bin included files that had been in the recycle bin since March 24, 2022. The data found in the information files is attached hereto as **Exhibit D-27**.

248. When a OneDrive user deletes files, copies of the files are placed into the recycle bin of the user's OneDrive account in the cloud. This is in addition to the recycle bin on the Windows computer. For example, when I reviewed the O365 Audit Log provided by Plaintiffs' counsel, I found that Ms. Grailer's deleted files were deleted from what is known as the "First-Stage Recycle Bin." Files deleted from the "First-Stage Recycle Bin" are automatically moved to the "Second-Stage Recycle Bin" without the end user's intervention. The Second-Stage Recycle Bin is not visible or accessible to end users such as Ms. Grailer, but site administrators can view and restore the files while they are stored there.[37] How long deleted files are stored in the Second-Stage Recycle Bin depends on the specific retention settings selected by the organization that controls the account. Deleted files may also be stored in the Second-Stage Recycle Bin indefinitely if the organization places a user's account on a litigation hold. I do not have knowledge of Plaintiffs' specific retention settings, or of whether or when Plaintiffs placed Ms. Grailer's account on a eDiscovery litigation hold in order to indefinitely preserve the deleted files still stored in her Second-Stage Recycle Bin. But these functions certainly were available to Plaintiffs, and such functions are typically used to ensure that files deleted by an end user are preserved and remain available to the organization and its system administrator for a period of time that the organization chooses.

[37] https://learn.microsoft.com/en-us/purview/retention-policies-sharepoint

249. Mr. Lieb did not mention any of the above functions in his report. He opined that Ms. Grailer deleted files and emptied her recycle bin on January 8, but he did not address the fact that the deleted files all should have been preserved and should have remained available in the Second-Stage Recycle Bin. (Lieb Report ¶¶ 20–21 & Ex. G.)

250. Mr. Lieb's Exhibit G also is misleading. Mr. Lieb claims that Ms. Grailer deleted all the files listed on Exhibit G from her laptop on January 8, 2023. (Lieb Report ¶ 20). That is clearly wrong in multiple respects.

251. First, many of the files listed in Mr. Lieb's Exhibit G—for example, the exhibit's first 10 rows—were stored in the INetCache folder. As I explained above, the INetCache folder is a hidden folder that is not managed by the user. Activity in the INetCache folder occurs behind the scenes. For example, when someone opens an attachment or adds an attachment to an email message, that attachment is automatically copied to the INetCache folder. Later, the copy is automatically deleted, all with no intervention from the user.

252. If you compare the first ten rows in Mr. Lieb's Exhibit G with Exhibit D-18 above, you can see that Mr. Lieb is simply listing "INetCache" copies of email attachments that Ms. Grailer received or sent through Outlook on January 8, 2023. When someone opens an attachment or adds to an attachment to an email message, that attachment is copied to the INetCache folder. Again, the INetCache folder is a hidden folder that is not managed by the user and this activity, including file deletion, occurs behind the scenes. An experienced and objective observer would understand right away that this has nothing to do with a user's deletion activities. The same type of activity occurs in the last 15 rows of Mr. Lieb's Exhibit G. That is application data (AppData), which is a hidden folder and not managed by the user, that is used by installed programs and the operating system. Mr. Lieb testified during his deposition that he knew that the INetCache folder is a system folder, not a place "that a user would go 'I'm going to open this up and interact or copy files to this location.'" (Lieb Dep. at p. 60.) Nonetheless, he included the INetCache folder's files in his Exhibit G.

253. Second, many of the files listed in Mr. Lieb's Exhibit G—all the files whose file names start with an "$R" prefix—are files that had been deleted at an earlier time and were

already present in the recycle bin. As explained above, when a user deletes a file, the file is moved from the original folder where it was stored to the user's recycle bin folder, and is renamed from the original file name to a new file name that starts with a $R prefix. As also noted above, such files had been accumulating in Ms. Grailer's recycle bin since March 2022. Some of the $R files in Mr. Lieb's Exhibit G derive from the files Ms. Grailer deleted on January 8, 2023. For example, you can find in Mr. Lieb's Exhibit G the "$RCEI1XS.docx" file that I discuss in paragraph 244 above. But the recycle bin also included many other $R files that derived from deletions going back to March 2022.

254. Third, Mr. Lieb also includes a large number of "$I" prefix files in his Exhibit G. For example, his Exhibit G lists the "$ICEI1XS.docx" file that I discuss in paragraph 244 above. It is difficult to understand how Mr. Lieb could have confused these $I prefix files for files that Ms. Grailer might have deleted. As explained above, when Windows moves a file to the recycle bin folder (and gives that file a new name starting with an $R prefix), it also creates an *additional* recycle bin information file containing the date and time when the $R file was deleted, the size of the file, and the original file name and folder where the file was stored. That additional recycle bin information file starts with an $I prefix. All the $I prefix files throughout Mr. Lieb's Exhibit G represent such recycle bin information files. These are obviously not files that the user deleted or even would have known about. An experienced and objective examiner would understand this immediately. During his deposition, Mr. Lieb testified that he knew that $I files would typically not be visible to a user like Ms. Grailer. (Lieb Dep. at pp. 207–208.) But again, he nonetheless included large numbers of $I files in his Exhibit G.

IV. PRESERVATION OF EVIDENCE

255. In Mr. Lieb's report (Lieb Report ¶ 10), he described how he used "Best Practices" and used "*tools and methodologies that do not make changes to the underlying electronic evidence in any way. If the proper standardized software is not used, it can result in the underlying data being changed or otherwise distorted.*"

256. Based on Lieb's report (Lieb Report ¶ 16), the Grailer Laptop was not accessible to Ms. Grailer after January 10, 2023. Based on Exhibit D to Mr. Lieb's report, it appears that Mr. Lieb's office took custody of the Grailer Laptop on February 8, 2023 at 11:03 AM.

257. I would agree that extracting the internal solid state drive from a laptop computer and using a Tableau TX1 hardware device to make a forensically-sound image of the solid state drive would be a good practice. According to the imaging log[38] for the Grailer Image, the imaging process started at 4:37:20 PM (CST). An excerpt of that log is depicted in **Exhibit C, Figure 26**.

258. Mr. Lieb failed to mention anywhere in his report that a significant amount of information had been altered on the internal solid state drive evidence after he took custody of the Grailer Laptop up to the time that he finally removed the hard drive to image it.

259. The Windows system event log showed that the Grailer Laptop started running on 2/8/2023 at 11:44 AM (CST). The computer continued to run at various times through the day.

260. Based on the registry and event log entries, two USB storage devices were connected to the Grailer Laptop while the computer was powered on. The event log entries are depicted in **Exhibit C, Figure 27**.

261. The security event log shows that Mr. Lieb also logged into a local administrator account (EcoAdmin) at 3:22 PM (CST). Since that account had not been used before, that action generated 5,055 new files and folders in the newly created user profile folder.

262. Examples of alteration consists of file system metadata, including over 197,000 instances of date and time stamps, the purging of USN change journal entries from before 1/8/2023 at 7:20:27 PM (CST), and alterations to the Windows registry. I also referenced some of this activity in Paragraph 139; Paragraph 149.a; and Paragraph 149.b. The activity is also depicted in Exhibits D-2, D-5, D-6, D-7, D-8, D-9, D-11, and D-21. After all of the alterations had occurred, Mr. Lieb finally removed the internal solid state drive and imaged it.

[38] LT001-JESSICA-GRAILER.log.txt

263. In my opinion, Mr. Lieb did not observe "Best Practices" in preserving digital evidence and this is clearly demonstrated by everything that was altered from the time he took custody of the Grailer Laptop.

264. During his deposition, Mr. Lieb claimed that he needed to use the Grailer Laptop computer because it was BitLocker encrypted and the serial number was not visible. (Lieb Dep. at p. 275.) His explanation of causing permanent changes to the data on the storage drive does not make sense. First, Bitlocker encryption does not prevent an examiner from creating a forensic image before conducting any type of analysis. When forensic software, such as Axiom, is used to access a forensic image containing Bitlocker, the software will display the Bitlocker Recovery ID and prompt the examiner to enter the Bitlocker Recovery Key. In this case, Ecolab needed simply to provide Mr. Lieb with the Bitlocker Recovery Key.

265. If the examiner needs any information from the original digital evidence, the examiner has the option of creating a working copy of the original evidence. This working copy can be made without altering the original evidence.

266. In Mr. Lieb's deposition, he stated "I had to perform a live forensic image." (Lieb Dep. at p. 275.) That statement made no sense since he actually created a forensic image by removing the storage drive from the laptop and creating an image with a Tableau TX1 hardware device. None of his actions on February 8, 2023 are reflected in the boilerplate language he used to describe his handling of the digital evidence or come anywhere close to his claim about using "best practices."

V. PROFESSIONAL TRAINING

267. During my review of this matter, I have had the opportunity to review Mr. Lieb's professional training certificates and courses that he shared as attachments to his declaration and expert report. The professional training and certificates he shared were based on introductory and intermediate level courses provided by forensic software vendors. While there is nothing wrong with these courses, they are vendor courses primarily designed to train the user on how to use the vendor's software, such as which buttons to push and a general overview of where the information is located. None of these courses would be considered advanced-level, which is

where the students are provided with in-depth instruction and information to conduct analysis, to interpret and support their findings, and to incorporate those findings into a timeline of events. I would consider some of the errors and omissions in Mr. Lieb's work product in this matter to be attributable to his lack of advanced-level training.

* * * * *

268. I am being compensated for my study and testimony in this case at the following rates: (i) $325 per hour for computer forensic analysis and associated services; (ii) $475 per hour for expert witness testimony and preparation. My fees are in no way dependent on my conclusions or on the outcome of this case.

Dated: February 2, 2024

BRUCE PIXLEY